Privacy in a House of Glass: Demanding Accountability for Spyware Use in Indonesia



ELSAM
LEMBAGA STUDI & ADVOKASI MASYARAKAT

Privacy in a House of Glass: Demanding Accountability for Spyware Use in Indonesia

Research Team:
Kezia Khatwani
Adzkar Ahsinin
Gurnadi
Parasurama Pamungkas
Nurul Izmi

Privacy in a House of Glass: Demanding Accountability for Spyware Use in Indonesia

Research Team:
Kezia Khatwani
Adzkar Ahsinin
Gurnadi
Parasurama Pamungkas
Nurul Izmi

Indonesian Edition Editorial Team:
Sungeb
Ferinda Khairunissa Fachri

Design & Layout:
Dodi Sanjaya
Samuel Johanes

First published in Indonesian by the **Institute for Policy Research and Advocacy (ELSAM)** in collaboration with **Seknas FITRA** and **FIND**

April 2026

CC BY NC SA

Table of Contents

Table of Contents	i
Foreword	1
A. Introduction	7
B. Research Questions	26
C. Research Methods	27
D. Device Characteristics, Spyware Operations, and Types of Threats to Targets	30
E. Spyware and the Interests of State Power: Spyware Operations in Various Countries	39
F. The Threat of Spyware to Democracy and Human Rights: The Construction of a Human Rights Norm Structure in Responding to the Dynamics of the Relationship between Technology and Human Rights	55
G. David vs. Goliath: The Powerless Public vs. the Gigantic Power of Technology Corporations in the Framework of the Business Norms and Human Rights Landscape	71
H. Challenges in Resolving Cases for Spyware Victims: Limitations of Existing Human Rights Protections in Providing Protection of Emerging Digital Rights	91
I. The Urgency of Developing a Human Rights-Based Accountability Ecosystem for Spyware Use in Indonesia	115

I.1. Legal Void Regarding the Use of Commercial Spyware and the Procurement of Commercial Spyware 115

I.2. Transparency Gaps in the Procurement of Goods and Services for Intelligence and Surveillance Technology 135

I.3. Traces of Spyware Use in Indonesia and Its Threats to Human Rights: Case Reflections 147

J. Postscript 161

J.1. Conclusion 161

J.2. Recommendations 162

Bibliography 161

Profile 181

Foreword

The development of information and communication technology in recent decades has brought fundamental changes to the way human beings interact, work, and construct social relationships. However, behind the progress, increasingly complex threats to the right to privacy and individual security have emerged. One increasingly prominent threat is the use of spyware, which allows for the collection of data covertly and invasively, often without user consent.

As demonstrated in various studies on privacy, surveillance practices are no longer limited to the context of state security but have expanded into various aspects of daily life. This phenomenon is further exacerbated by the emergence of spyware technology, which can access almost all of a person's digital activities, from private communications to location data, in a real-time basis. In many cases, the use of this technology raises not only technical issues but also touches on the dimensions of human rights, democracy, and power relations.

This research aims to provide a more comprehensive understanding of spyware, including its characteristics, working mechanisms, and implications for privacy and civil liberties. Furthermore, this research also seeks to examine how the practice of spyware use has evolved in both global and national contexts, and the extent to which existing legal frameworks are able to anticipate and control potential abuse.

In a broader context, the increasing use of surveillance technology indicates a shift in the relationship between individuals, the state, and corporations. Massive data collection and opaque surveillance practices have the potential of creating a power imbalance, with individuals increasingly losing control over their personal information. Therefore, it is important to position the issue of spyware not solely as a technological issue, but also as part of the discourse on human rights and digital governance.

Therefore, this research is expected to contribute to the development of a

critical understanding of spyware and encourage broader discussions on the importance of privacy protection in the digital age. With increased public awareness and the strengthening of human rights-oriented regulations, it is hoped that the use of surveillance technology can be controlled more accountably and transparently.

Genealogy of a Metaphor: Privacy in a House of Glass

The title "Privacy in a House of Glass" is a literary device that is highly relevant to today's conditions. It is inspired by Pramoedya Ananta Toer's fourth novel in the Buru Quartet, "House of Glass" (1988), which chronicles the systematic surveillance carried out by the Dutch colonial state on Minke, the main character representing the early nationalist movement in the Dutch East Indies.

In the novel, the "House of Glass" becomes a powerful metaphor for the condition of someone living under the inescapable gaze of power, where every movement is recorded, every word is recorded, every relationship is mapped by the colonial intelligence apparatus. Minke is never truly free, for his freedom is only an illusion within a surveillance structure that is transparent from the outside but constricting from the inside. He can see the world, but the world, or more precisely, power, also constantly sees him.

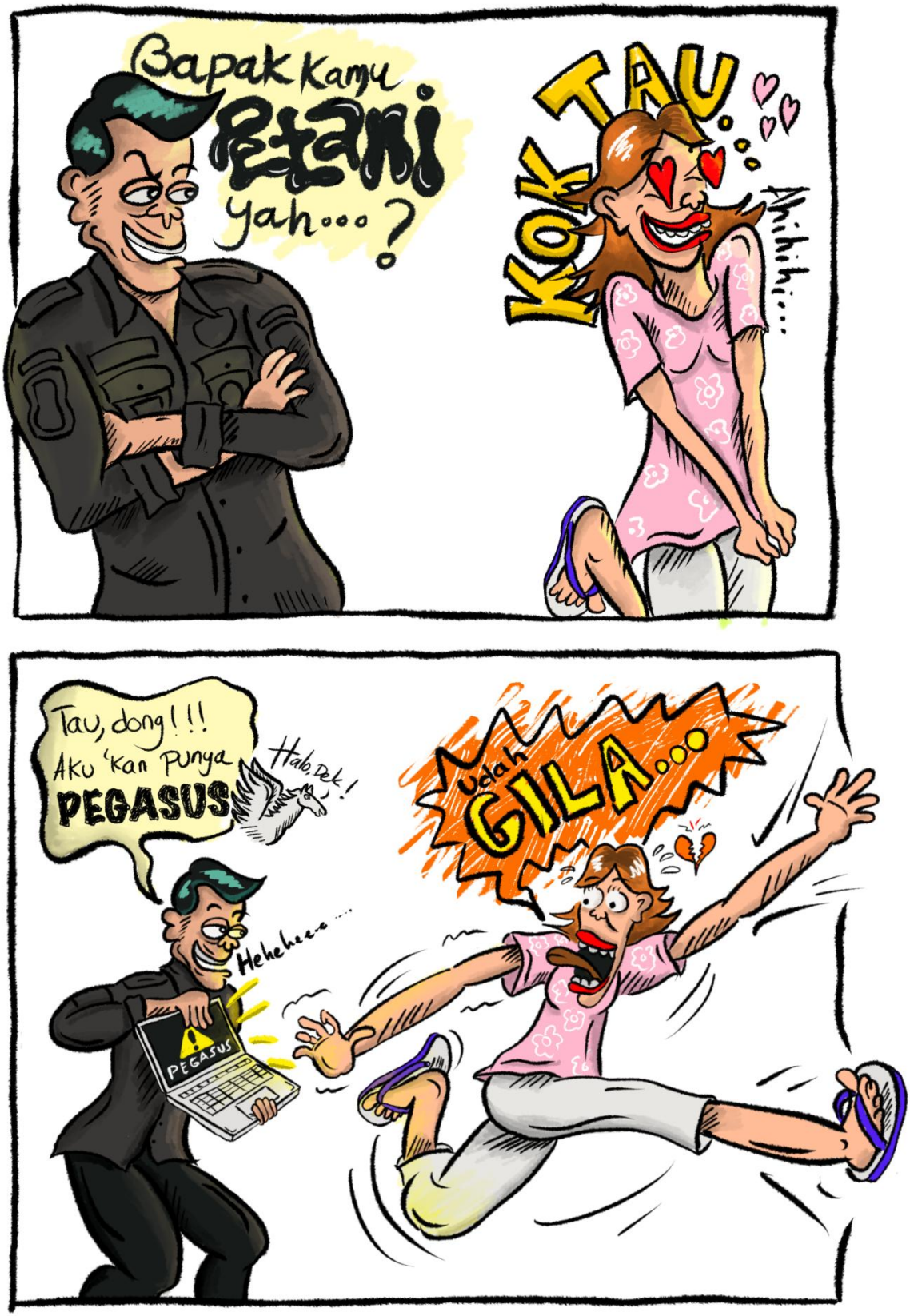
More than a century after the setting described by Pramoedya, Minke's condition feels more than just history. Today's spyware technology replicates the logic of the "house of glass" in the palm of our hands; devices we thought were tools for freedom can actually become windows that allow others to peek in without our knowledge. The names are different, the technology is different, but the relationship between the monitor and the monitored remains structured similarly: a deep asymmetry of power, where one party has full visibility while the other is unaware of being observed.

Borrowing Pramoedya's image, this research aims to emphasize that the issue of digital surveillance is not a new phenomenon born of silicone sophistication. It is the continuation of a long genealogy of power—the desire to see, know, and control. Calling it "Privacy in a House of Glass" is a reminder that

we are not dealing with a purely technical issue, but rather with something much older and deeper—a struggle between the right to be invisible and the power desire to not miss a thing.

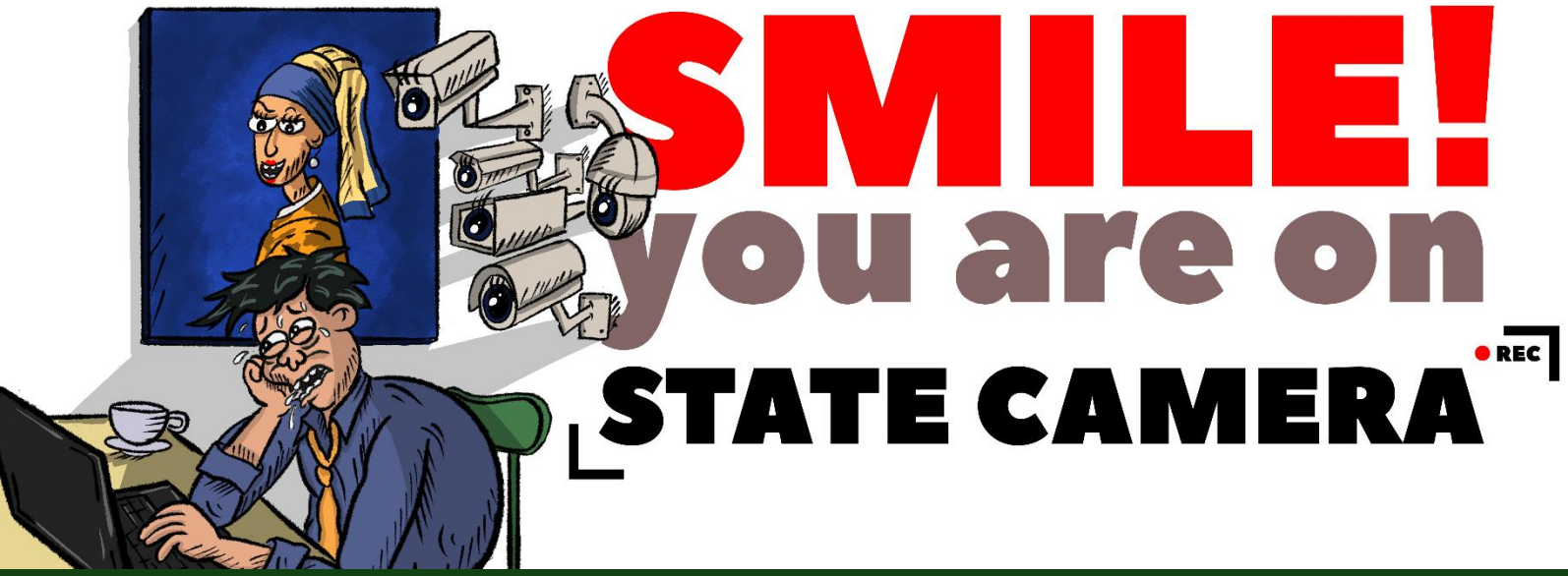
Furthermore, this research is expected to contribute to the development of a critical understanding of spyware and encourage broader discussion on the importance of privacy protection in the digital age. With increased public awareness and strengthened human rights-oriented regulations, it is hoped that the use of surveillance technology can be controlled more accountably and transparently.

Desiana Samosir
Executive Director
Institute for Policy Research and Advocacy (ELSAM)


Bapak Kamu Pejabat yah...?
KOK TAU..
Ahihihi...
Tau, dong!!!
Aku 'kan punya PEGASUS
Halo, Dek!
Udah GILA...
Hehehee...
PEGASUS

"You might be free, but under my surveillance."

– Pramoedya Ananta Toer, *House of Glass* (1988)


SMILE!
you are on
STATE CAMERA
REC

"We've got agencies looking through webcams into people's bedrooms, and they're collecting billions of cell phone locations records a day. They know where you got on the bus, where you went to work, where you slept, and what other cell phones slept with you."[1]



Edward Snowden

A. Introduction

Governments around the world are intensifying repression against critical voices by targeting human rights defenders, journalists, and activists through targeted digital surveillance. This practice involves hacking devices designed to hinder humanitarian activities, ultimately undermining democratic principles and the rule of law. As an increasingly predominant tactic, such surveillance has become a primary tool for states to widely and systematically suppress dissent, particularly through the use of spyware such as NSO Group's Pegasus and similar technologies. Spyware is a powerful and flexible technique that poses a unique and serious threat to privacy and security.[2] In 2021, Forbidden Stories and Amnesty International, through the Pegasus Project, gained access to a list of 50,000 phone numbers selected as targets by NSO Group clients. Analysis of this list revealed the identities of more than 1,000 individuals across more than 50 countries. The targets included prominent figures, including members of Arab royal families, 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials, including cabinet ministers, diplomats, and military and security personnel.[3]

---

[1] Amnesty International UK, "Evidence of Global Opposition to US Mass Surveillance," 16 January 2026, https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq. Accessed on 16 December 2025

[2] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure" (Amnesty International Ltd, 2021).

[3] Steven Feldstein and Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*, Carnegie Endowment for International Peace, 14 March 2023, https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses.

Pegasus, NSO Group's flagship product, is currently perhaps the most sophisticated form of spyware on the market. This software can remotely collect all data from a target device, including photos and videos, files, text messages, contacts, and call logs. The software can control the smartphone's camera and microphone to see and listen to the target, as well as monitor its location, log keystrokes, and eavesdrop on phone or video calls.[4]

In its development, surveillance devices are no longer limited to controlling various applications on smartphones. In more extreme cases, they can be misused as tools to target civilians, such as the killing of tens of thousands of civilians in Gaza, Palestine. The genocide in Palestine proves that spyware is a weapon of war that threatens not only Palestinians in Gaza, but all of humanity.[5] Israeli companies such as NSO Group, Candiru, Intellexa, Paragon, and others have created military-grade spyware, such as Pegasus, Predator, and Graphite, that can infiltrate mobile phones, extract personal data, and even turn them into surveillance devices. This technology has reportedly been field-tested on Palestinians by Israeli intelligence units before being commercialized and marketed globally. Spyware is a weapon used by authoritarian regimes and self-proclaimed "democratic" regimes to silence dissent and opposition, target journalists and lawyers, and tear apart the fabric of human rights values.[6]

These new surveillance technologies, largely developed by private companies, are unregulated and opaque. This critical vulnerability allows hackers to remotely infiltrate smartphones without the knowledge of the targeted individual. Once inside the phone, Pegasus can activate the camera and microphone and steal data, including communications, images, and videos. These weapons conduct targeted and invasive surveillance on a scale unimaginable before the advent of these tools. Israel's spy software industry has

---

[4] Mike Sexton, "What Is Spyware and Why Should Policymakers Care?," *Third Way*, 9 March 2023, https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care. Accessed on 6 August 2025

[5] "The Dangerous Rise of Military-Grade Spyware – a Global Day of Action," *BDS Movement*, 18 June 2025, https://bdsmovement.net/Global-Day-Action-Against-Spyware. Accessed on 31 December 2025.

[6] "The Dangerous Rise of Military-Grade Spyware – a Global Day of Action."

profited from the surveillance of every aspect of Palestinian life. The private sector has subsequently used this experience as a basis for designing, developing, and exporting these technologies worldwide, to both democratic and authoritarian states. Palestinians in the occupied territories are often used as guinea pigs in the development and testing of Israeli military technology. Spy software is a central part of this picture. Technology tested on Palestinians is then marketed globally with claims of being "battle-tested" to attract international buyers.[7]

This situation highlights the increasing surveillance risks associated with the adoption and use of spyware technology in the coming years. At the same time, as this technology becomes commercially available and its use by governments expands, organizations and individuals will likely struggle to prevent and identify spyware on their devices.[8]

According to data from the Carnegie Endowment for International Peace, at least 74 governments contracted with commercial companies to acquire spyware or digital forensics technology between 2011 and 2023. Autocratic regimes were significantly more likely to purchase commercial spyware or digital forensics software than democracies. This trend is evident in the contractual relationships in which 44 regimes classified as closed autocracies or electoral autocracies acquired targeted surveillance technology between 2011 and 2023, compared with 30 electoral democracies or liberal democracies.[9] Dragonfly Intelligence's findings reinforce the growing trend of authoritarian governments targeting individuals working in journalism and civil society organizations (NGOs) with spyware. Spyware is typically distributed through *spear-phishing* tactics, in which victims are sent messages containing malicious links designed to infect their devices. Authorities in many countries have likely already utilized spyware technology aimed at individuals or organizations working on issues deemed

---

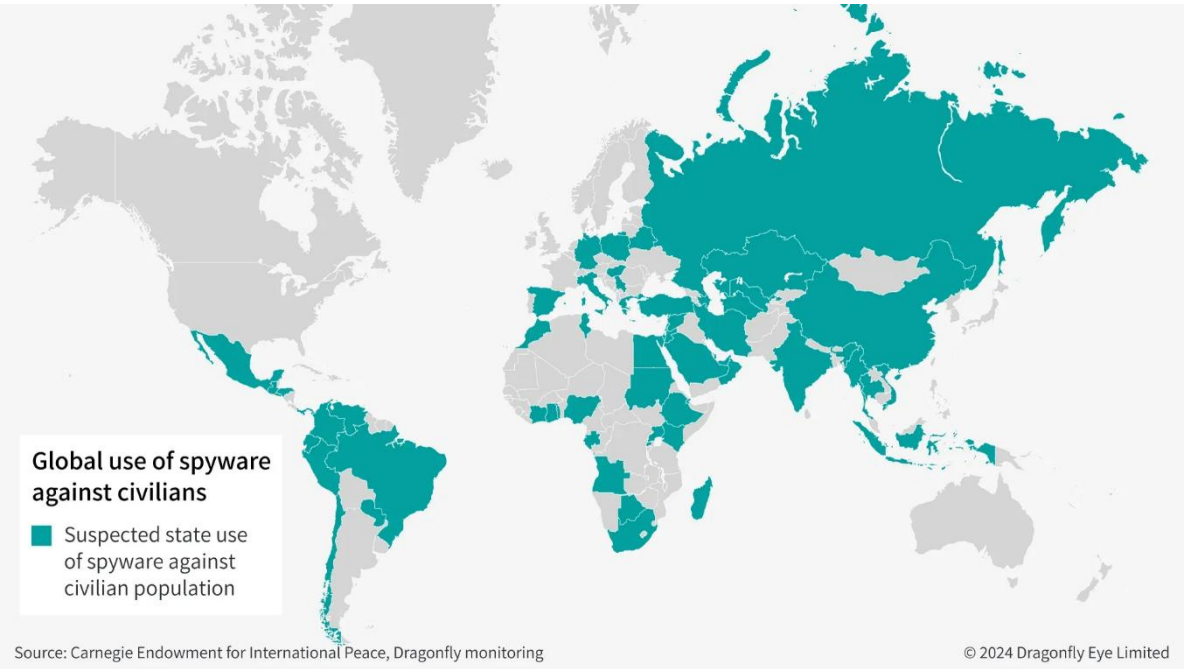
[7] Antony Loewenstein, "How Palestine Became Israel's Spyware Test-bed," *New Internationalist*, 19 October 2023, https://newint.org/features/2023/10/02/spy-games. Accessed on 31 December 2025.

[8] "Risks to organisations from spyware," Dragonfly Intelligence, 27 June 2024, https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/. Accessed on 31 December 2025

[9] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*

politically sensitive by authoritarian governments, such as human rights, political asylum seekers, or corruption. According to Dragonfly Intelligence analysis, Azerbaijan, Egypt, Indonesia, Jordan, Kazakhstan, and Saudi Arabia are identified as highly motivated to use spyware against individuals and organizations in the coming years.[10]

The map below shows countries suspected of misusing spyware for politically motivated intelligence surveillance of civilians. It is based on a dataset on commercial spyware use and CitizenLab research.[11]



Support from a broad customer base of governments in the global market strengthens the position of these software providers, despite various regulatory efforts targeting the spyware supply chain. The commercialization of the spyware industry is reflected in the following facts:[12]

---

[10] Dragonfly Intelligence, "Global Risks to Organisations from Spyware," *Dragonfly Intelligence*, 24 June 2024, https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/. Accessed on 13 August 2025

[11] Dragonfly Intelligence, "Global Risks to Organisations from Spyware."

[12] Jen Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights" (Atlantic Council, 4 September 2024).

1) Of the 195 countries in the world, at least 80 countries are known to have purchased spyware from commercial vendors;
2) As many as 14 of the 27 European Union member states were identified as having purchased spyware from a single vendor, namely the NSO Group;
3) Spyware vendors were indicated to be involved in 50 percent of the total zero-day exploits throughout 2023. This figure includes 64 percent of all exploits targeting mobile software and browsers;
4) While the industry's annual revenue is difficult to pinpoint, the economies of scale are enormous; one vendor has even considered an IPO valuation of $2 billion.

Israel is a major exporter of spyware technology and digital forensic tools recorded in the global inventory database. Fifty-six of 74 governments have purchased commercial spyware and digital forensic technology from companies based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox, and Candiru. In addition to the top commercial spyware vendors like NSO Group and Cytrox, a secondary layer of suppliers has developed, including specialist spyware companies, mercenary hacking operations, exploit brokers, and other similar entities. As large commercial companies face increased scrutiny from democratic governments, there is simultaneously a growing demand for open-source and commercially available malware. This trend has made spyware technology cheaper for both governments and private actors to conduct attacks and allows them to hide in the "noise" of open-source spyware code.[13] Furthermore, Israel, as a leading spyware exporter, has not sufficiently prioritized human rights considerations in its export licensing regime.[14]

The surveillance industry operates in secret, despite repeated calls for greater transparency and accountability. This lack of transparency poses a fundamental challenge to holding people accountable for human rights

[13] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*
[14] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*

violations arising from the use of spyware. Without more information about the surveillance industry, such as (1) the jurisdictions in which it operates; (2) the identity and ownership of the companies facilitating government surveillance; (3) the capabilities offered; (4) the scale of deployment; or (5) details of the companies' due diligence or remedial efforts, it is impossible to ascertain the full scope of human rights risks, mitigate them, or seek redress when violations occur. The UN Special Rapporteur on freedom of opinion and expression noted in her 2019 report that there are substantiated allegations that many companies sell surveillance tools to governments to spy on journalists, activists, opposition figures, and others who play a crucial role in democracy. Due to the serious nature of these allegations, companies are required to be transparent about who they do business with and how they operate.[15]

Furthermore, the global spyware and digital forensics industry has strengthened the capacity of both democratic and authoritarian governments to conduct advanced intrusions. The Carnegie Endowment for International Peace identified key vendors and clients in the global spyware industry and highlighted the links between governments and intrusion software suppliers.[16] According to Carnegie Endowment for International Peace data, Indonesia has been using spyware produced by the German firm FinFisher since 2015. This spyware was used to persecute religious minorities and LGBT groups. Furthermore, between 2021 and 2022, Indonesia also used products from Candiru, NSO Group, and Cytrox, all Israeli firms. Previously, in 2020, in addition to spyware, Indonesia also used digital forensics technology produced by Israeli firm Cellebrite.[17] Indications of the use of spyware in Indonesia were also revealed by the IndonesiaLeaks Consortium, whose members include Tempo, the global journalist network

[15] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."
[16] Steven Feldstein and Brian Kot, "Mapping the Shadowy World of Spyware and Digital Forensics Sales," *Carnegie Endowment for International Peace*, 27 February 2023. https://carnegieendowment.org/features/commercial-spyware?lang=en. Accessed on 31 December 2025
[17] Feldstein and Kot, "Mapping the Shadowy World of Spyware and Digital Forensics Sales."

Forbidden Stories, and the Organized Crime and Corruption Reporting Project (OCCRP), which discovered the Pegasus spyware operation in Indonesia.

Amnesty International's research confirms the existence of Pegasus that threatens civil space in Indonesia. The study found that the Indonesian National Police (Polri) and the National Cyber and Crypto Agency (BSSN) imported spyware technology from Israel, Greece, Singapore, and Malaysia between 2017 and 2023. Suppliers of spyware technology to Indonesia include Q Cyber Technologies, which is linked to the NSO Group, the Intellexa consortium, Saito Tech (Candiru), FinFisher and its subsidiary Raedarius M8 Sdn Bhd, and Wintego Systems. These state institutions procured surveillance technology and spyware through intermediary companies based in Singapore. The listing of third parties as administrative owners in these official documents creates serious obstacles in identifying the true owners. The use of this legal structure complicates the verification of the surveillance technology supply chain. This opacity cripples oversight in the public procurement process, as the identities of the original vendors become difficult to trace.[18]

In addition to NSO Group's Pegasus, Cytrox's Predator spyware has become a favorite choice for many governments and was recently the subject of an investigation in Greece, following revelations that government operatives used Predator malware to hack the phones of journalist Thanasis Koukakis and opposition leader and member of the European Parliament Nikos Androulakis. In addition to Greece, state-backed operatives in Armenia, Côte d'Ivoire, Egypt, Indonesia, Madagascar, Serbia, and Spain also likely use Predator.[19] This highly invasive spyware is designed to be covert, leaving minimal footprints, making it extremely difficult to detect. Further, this situation risks creating deliberate impunity for violations of rights such as the rights to freedom of expression, peaceful assembly and association, security of person, and freedom from

[18] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia," 2024.
[19] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

arbitrary detention.[20] Meanwhile, many countries lack robust legislative frameworks to protect citizens who could potentially fall victim to the misuse of this highly invasive spyware and other surveillance technologies.[21] "Until now, Indonesia has not had a specific legislative framework governing the legality of using spyware and surveillance technology. The most relevant regulations currently remain limited to the wiretapping provisions for law enforcement, as stipulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), which has been amended several times, most recently through Law Number 1 of 2024.[22]

The scope and variety of surveillance technologies available today are unprecedented in human history, allowing for the monitoring and tracking of individuals or groups on a massive scale, including the location, communications, and browsing histories of individuals. This expanding scope of surveillance is enabled by recent leaps in digital technology capabilities and fueled by global events, such as the Covid-19 pandemic. According to Neil M. Richards, humanity is now entering an age of surveillance.[23] The use of surveillance technology is no longer dominated by authoritarian states but has also expanded into democratic countries. This phenomenon creates global risks to privacy and human rights, as intense surveillance now occurs in nearly all forms of government. Mass surveillance is also no longer limited to intelligence agencies. It is embedded in public-private partnerships, consumer platforms, and smart cities, often implemented without adequate legal oversight or meaningful public debate. From facial recognition cameras on city streets to predictive policing algorithms targeting specific populations, surveillance technology has reached a pervasive level that challenges the boundaries of human rights protections. The post-

[20] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.

[21] Amnesty International, "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia."

[22] According to this law, wiretapping is the activity of listening to, recording, diverting, changing, blocking and/or recording the transmission of electronic information and/or electronic documents that are not public, either via wired communication networks or wireless networks, such as electromagnetic radiation or radio frequency transmissions.

[23] Neil M. Richards, "The Dangers of Surveillance," *Harvard Law Review*, Vol. 126:1934, 2013, p. 1936

Edward Snowden era has sparked global awareness of state-driven surveillance practices. However, a decade later, private actors have become equally important in building and maintaining global digital surveillance infrastructure. Commercial surveillance devices are sold to governments with a poor record of human rights violations, and multinational corporations collect, share, and monetize personal data on an unprecedented scale. Surveillance is no longer an exceptional tool used in high-risk contexts. It has become routine, normalized, and often opaque.[24]

The primary rationale for the use of surveillance technology has long been based on the promise of increased security. Governments and private actors often defend the use of biometric scanners, facial recognition systems, and artificial intelligence-based surveillance devices as necessary responses to terrorism, crime, and social unrest. This justification, built on the freedom-versus-security dichotomy, simplifies a highly complex issue and obscures the evolving role of surveillance in contemporary society. As digital infrastructure expands, surveillance capabilities are growing not only in scale but also in purpose, no longer confined to counterterrorism or law enforcement. Surveillance, in practice, now also serves a variety of administrative, commercial, and political purposes. This shift requires a reframing of the debate as surveillance not only as a security tool but also as a control mechanism. Furthermore, the use of surveillance for social and behavioral engineering is increasingly evident in both democratic and authoritarian regimes. Artificial intelligence-based systems are being used to detect "pre-crime" behavior, assess creditworthiness, manage welfare access, and suppress dissent. These functions, while presented as governance tools, often rely on opaque algorithms and unregulated data collection practices that erode public trust and reduce individuals to data points in a risk matrix.[25]

The spyware industry has become one of the greatest threats to civil society, human rights, and democracy today. This phenomenon emerges amidst efforts

[24] Edmarverson A. Santos, "Human Rights and the Global Digital Surveillance Infrastructure," *Diplomacy and Law* (blog), 3 July 2025, https://www.diplomacyandlaw.com/post/human-rights-and-the-global-digital-surveillance-infrastructure. Accessed on 16 December 2025

[25] Santos, "Human Rights and the Global Digital Surveillance Infrastructure."

by various countries to confront the proliferation of invasive surveillance instruments operating without adequate regulation.[26] The use of surveillance technologies such as spyware not only poses the risk of immediate violations of the rights to privacy, freedom of expression, and freedom of peaceful assembly, but also hinders people from exercising those rights in the future. Spyware technology is a type of malicious software used to collect information from a device without informing the user and transmitting it to unauthorized entities. This technology is highly invasive because it allows unrestricted access to a device automatically and leaves very little trace, making it nearly impossible for the user to determine what data has been collected.[27]

Spyware technology is often referred to as lawful interception technologies, a logical consequence of which is that these products are highly vulnerable to misuse. However, to date, there is no framework to prevent such misuse, and no consequences for its use. Companies selling highly dangerous technologies have largely escaped punishment. This situation demonstrates the need for proper regulation of the use of spyware technology, guided by human rights principles, to ensure that rights violations do not recur.[28]

Michel Foucault's theory on surveillance is constructed around the relationship between knowledge and power, and the construction of truth through archiving. This approach offers a relevant lens for uncovering the structures of control embedded in digital evidence practices. David Lyon defines surveillance as focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction. Surveillance creates a relationship between the authority (principal) and the individual (subject) monitored through the surveillance gaze. This condition triggers anticipatory behavioral patterns, where the subject proactively adjusts their

[26] Leyland Cecco, "Spyware Is Huge Threat to Global Human Rights and Democracy, Expert Warns," *The Guardian*, 10 August 2022, https://www.theguardian.com/world/2022/aug/09/spyware-canada-threat-democracy-human-rights. Accessed on 6 August 2025

[27] Amnesty International, A Web of Surveillance: Unravelling A Murky Network Of Spyware Exports To Indonesia, p. 7.

[28] Amnesty International, "When Is Targeted Surveillance Wrong?," 10 August 2023, https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/. Accessed on 16 December 2025.

actions to align with the authority's expectations and self-censors behavior deemed undesirable. Michael Foucault's concept of the panopticon, derived from Jeremy Bentham's prison design, centers on the internalization of control through surveillance. The use of this framework is important because surveillance is neither passive nor neutral. Carissa Véliz states that the application of surveillance to an individual is a manifestation of domination. In other words, surveillance is closely linked to systems of oppression, including racism and colonialism. Surveillance theory addresses the power dynamics implicit in digital evidence: the power held by those in authority to determine, through algorithms and other incentives, what information is prioritized, valued, and even considered true. Meanwhile, the experiences of targeted individuals reflected in digital evidence may be deprived of their rights. The harm and suffering embodied in digital evidence and digital content receive no meaningful response. The international legal system remains unresponsive in the face of overwhelming evidence. This phenomenon indicates that control over digital evidence and content has become an instrument of global power, creating its own form of domination.[29]

In certain circumstances, the use of invasive surveillance techniques may be justified, such as to prevent or investigate certain serious crimes or acts that pose a serious threat to national security. International law states that targeted surveillance measures must be strictly tailored to investigate specific individuals suspected of committing serious crimes or acts that threaten national security. Spyware should be used as a last resort, after all less invasive measures have been exhausted or have proven ineffective. However, the duration and scope of spyware use must be strictly limited to relevant data. In other words, governments

[29] Chris Carpenter, "Symposium on Forensic and Counter-Forensic Approaches to International Law: Digital Evidence and the Gaze – a Conceptual Framework for Analyzing Digital Evidence Through a Foucauldian Lens," Opinio Juris, 16 March 2026, https://opiniojuris.org/2025/12/10/symposium-on-forensic-and-counter-forensic-approaches-to-international-law-digital-evidence-and-the-gaze-a-conceptual-framework-for-analyzing-digital-evidence-through-a-foucauldian-lens/. Accessed on 16 December 2025.

must adhere to the principles of legality, necessity, and proportionality when using surveillance technology.[30]

However, the reality is that governments rarely adhere to these standards. States continue to exploit national security or public order concerns to grant law enforcement agencies broad discretion to use invasive software against a wide range of targets, with little regard for the principles of necessity and proportionality. Once these agencies acquire spyware, there are few safeguards in place to regulate its use. David Kaye, the UN special rapporteur on freedom of opinion and expression, said:[31]

"It's not enough to say that a comprehensive system for controlling and using targeted surveillance technology is broken. It's virtually non-existent. Despite human rights law providing clear limits on the use of surveillance devices, states continue to conduct illegal surveillance without fear of legal consequences. A human rights legal framework exists, but a framework for enforcing those limits does not."

In this context, the UN Special Rapporteur on the right to freedom of peaceful assembly and of association stated:[32]

"For many people in civil society, the internet is no longer a safe haven, as they have become targets of increased surveillance and online violence. These actions are often carried out by state agents but facilitated by private internet service providers."

After years of accumulating evidence demonstrating the negative impact of digital surveillance technology on human rights, from reports of the use of French company Amesys surveillance equipment in Libya during the Arab Spring to recent revelations of the targeting of journalists globally, the UN Special

[30] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.
[31] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*.
[32] International Commission of Jurists, "Digital Technologies and Human Rights: a Legal Framework" (International Commission of Jurists, May 2022), p. 4.

Rapporteur on freedom of opinion and expression recently concluded that the surveillance industry continues to provide its services without oversight and with near impunity.[33]

There are several legal approaches according to George T. Papademetriou to limit the ability of private surveillance companies to facilitate human rights violations.

1) Strengthening the application of international human rights instruments to privacy protection.
2) Tightening domestic oversight through export controls and sanctions: Creating stronger national law enforcement mechanisms through export control regimes and the implementation of criminal sanctions for technology misuse.
3) Expanding access to redress for victims: Opening greater opportunities for victims to claim compensation at the domestic level through civil lawsuits (litigation) against vendors or related companies.

These core human rights instruments predate the revolutionary development of internet technology and did not anticipate the transformative impact that global communications would have on everyday life. More recent efforts to update human rights law to address these changes have made some progress in addressing these gaps, including highlighting the importance of the right to privacy in the digital technology ecosystem.[34] Furthermore, the

[33] Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."

[34] In 2015, the Office of the High Commissioner for Human Rights established a Special Rapporteur on the Right to Privacy, whose aim was to "raise awareness of the importance of promoting and protecting the right to privacy, including by taking into account the particular challenges arising in the digital age." Human Rights Council resolutions in 2017, 2018, and 2019 laid the groundwork for the groundbreaking General Assembly Resolution on Privacy in the Digital Age in 2020. This resolution identified several specific concerns about privacy in the digital context, including the need for states to maintain adequate oversight mechanisms that ensure accountability for state surveillance of communications, and to provide effective remedies when violations occur. The UN General Assembly emphasized the crucial role that businesses play in safeguarding the right to privacy and called on businesses that collect data to fulfill their responsibilities to respect privacy in accordance with the "Protect, Respect and Remedy" Framework. UN Guiding Principles on Business and Human Rights. See, George T. Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," Harvard Human Rights Journal 36 (2023), pp. 205-206

development of international legal protections faces additional challenges related to implementation within domestic law. While several documents, including the 2019 Report of the Special Rapporteur on Freedom of Expression, David Kaye, have affirmed that governments using surveillance tools have an obligation to ensure their use complies with domestic legal frameworks that meet the standards required by international human rights law, even if formally reflected in domestic law, the impact of international human rights obligations on individuals will depend on the strength of the rule of law and judicial independence, which vary across countries, given the tendency of intelligence agencies to operate clandestinely and with limited oversight.[35]

Meanwhile, there has been no international consensus on how governments should balance privacy with security to address existing legal gaps. Efforts to close these legal gaps are urgent for the international human rights community for two reasons:[36]

First, while the internationally recognized right to privacy creates certain legal obligations for states, these obligations are currently loose and leave considerable room for variation in state practice. A more stringent set of authoritative interpretations (for example, by updating General Comment 16 on the right to privacy) would provide the international community with an important tool to identify and condemn governments and companies that violate the right to privacy.

Second, if these efforts fail to create an internationally binding legal instrument, the articulation and contestation of the right to privacy and its

[35] Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," pp. 206-208.

[36] David Kaye and others involved in the international debate on how states can comply with their privacy obligations are engaging and participating in forums such as the Human Rights Council or the UN Group of Governmental Experts for Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, providing a space for governments to discuss thorny issues and reach consensus on the troubling role of surveillance technology companies in facilitating human rights abuses. This dialogue can, in turn, translate into state practice, including through authoritative interpretative statements from governments. While somewhat limited by states' willingness to violate norms when national security issues are at stake, the practical effects can still be significant. See, Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

attendant obligations in international forums have important normative effects. Transnational legal process theory argues that international human rights law, despite its lack of enforcement, shapes state behavior in three phases: interactions between states in which global norms are debated, interpretation of relevant legal principles, and internalization by domestic legal systems.

Furthermore, domestic export controls and criminal sanctions provide another set of mechanisms to control those who abuse spyware technology. Efforts to control exports and impose sanctions have a more direct impact on the profitability of spyware companies than international human rights instruments. However, several factors limit the transformative potential of this approach. First, export control regimes are potentially contested by political interests rather than a principled commitment to human rights. Second, relying solely on the state as law enforcer is problematic because bureaucratic and institutional considerations make it impossible to sanction private actors with ties to that state.[37]

These difficulties reflect the deep tensions in the relationship between privacy and security and reveal that relying on a single country to act as a global enforcer is not a sustainable solution. A more practical and related concern is the resource challenges posed by law enforcement. Maintaining a robust regulatory regime depends on the capacity to investigate, assess, and prosecute spyware companies that violate human rights. This, in turn, depends on the allocation of political funding.[38]

Neil M. Richards identifies four principles that guide the development of surveillance law in the future to create a balance between the costs and benefits

[37] For example, in the United States, in the Edward Snowden case, despite being a key catalyst for legal challenges to the program and its eventual conviction, law enforcement in the United States has a strong incentive to maintain relationships with private contractors. Reports indicating that the Federal Bureau of Investigation has tested NSO Group products and the CIA continues to conduct surveillance on US soil are important reminders that these law enforcement agencies often choose less privacy in the name of national security. See, Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

[38] Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry."

of government surveillance. First, surveillance transcends the public/private boundary. Public and private surveillance address the same issue, not entirely separate ones. Even if the focus ultimately falls on government surveillance, any solution must address the complex relationship between government and corporate surveillance. Second, unauthorized covert surveillance and the creation of any domestic surveillance program whose existence is kept secret should be legally prohibited. Third, total surveillance is illegal, and the government's intention to record all internet activity without authorization should also be legally prohibited. Government surveillance of the internet can lead to abuses of power and invade fundamental liberties. In this context, like wiretapping, surveillance must undergo a judicial process before it can be authorized. Fourth, surveillance is dangerous because it threatens intellectual privacy and increases the risk of blackmail, coercion, and discrimination. Therefore, surveillance is dangerous because it violates the constitutionality of fundamental civil liberties.[39]

Targeting human rights defenders through digital surveillance because of their opinions or work is never permissible under human rights law. It violates the right to privacy and hinders the exercise of freedom of opinion and expression, regardless of whether the targeted individual's data or communications are actually intercepted. It is often difficult to prove that such surveillance is taking place and that digital devices or personal data are being infected. Attempted spyware infections of targeted human rights defenders indicate that human rights defenders have been subjected to surveillance now or in the future. This suggests the need for governments to establish due diligence and protection measures through legal frameworks, as existing legislation and regulations are inadequate. At the same time, attempts to infect human rights defenders' digital devices indicate a failure on the part of the companies supplying the software, the governments of the companies' countries of origin, and the countries where

[39] Richards, "The Dangers of Surveillance," pp. 1935-1936.

the surveillance occurs to address the misuse of spyware.[40]

The Global Justice Clinic, New York University School of Law, emphasizes that states need to exercise restraint and protect human rights defenders from such unlawful rights violations by:[41]

1) Ensuring an adequate legal framework exists to authorize such targeting, subject to independent judicial review;
2) Enacting and enforcing export control laws that prevent the sale of malicious software and other forms of digital weapons to governments that do not have such minimal legal protections under their domestic laws; and
3) Conducting robust due diligence to ensure, at a minimum, that government purchasers of such software have those basic legal protections, providing a legal basis for targeting specific individuals with surveillance software and providing individuals with procedural protections against wrongful targeting.

In the Indonesian context, Amnesty International, through its research, has documented the use of spyware to target specific individuals. Although Amnesty International acknowledges it has no evidence that spyware has been used to target specific members of civil society, this difficulty stems from the inherently secretive nature of spyware, making it difficult to detect cases of misuse. Therefore, this situation risks creating impunity for human rights violations resulting from the misuse of these devices. Amnesty International places particular emphasis on the purchase of spyware in Indonesia, given that civil space has shrunk as a result of ongoing attacks on the rights to freedom of expression, peaceful assembly and association, personal security, and freedom from arbitrary detention. Furthermore, the lack of transparency in the procurement of spyware is fundamentally inconsistent with human rights, and

[40] Global Justice Clinic, "Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights," 1 March 2019, p. 3.
[41] Global Justice Clinic, "Attempted Digital Surveillance as a Complete Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights."

therefore, its procurement should be prohibited.[42]

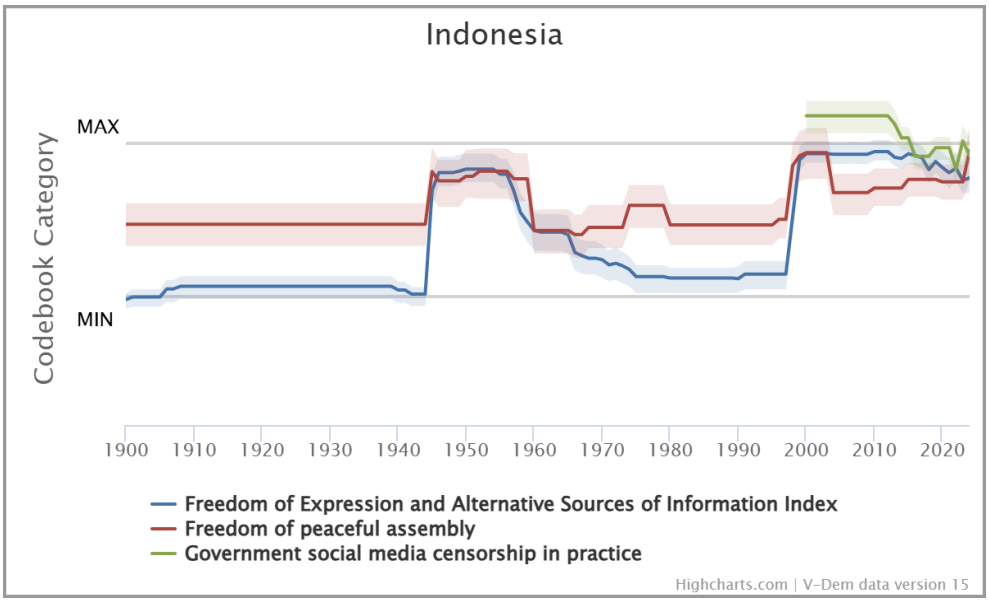
Based on the preliminary description above, this study attempts to analyze the use of spyware by the Government of the Republic of Indonesia, the use of spyware needs to be placed on the tendency of democratic decline in 2024. Indonesia has begun to move towards democratization after 1998 along with the fall of President Soeharto's regime and continued until the end of the 2000s. However, in the decade of President Joko Widodo's administration (2014-2024) Indonesian democracy continues to experience decline marked by increasing polarization and illiberalism. According to the V-Dem Institute, this situation indicates a transition from an electoral democracy since 1999 to an autocratic gray zone by 2024.[43]

The downward trend in democracy in Indonesia can at least refer to threats to freedom of expression, freedom of peaceful assembly, and freedom of expression on the Internet without censorship, referring to V-Dem Institute data as seen in the diagram below.[44]

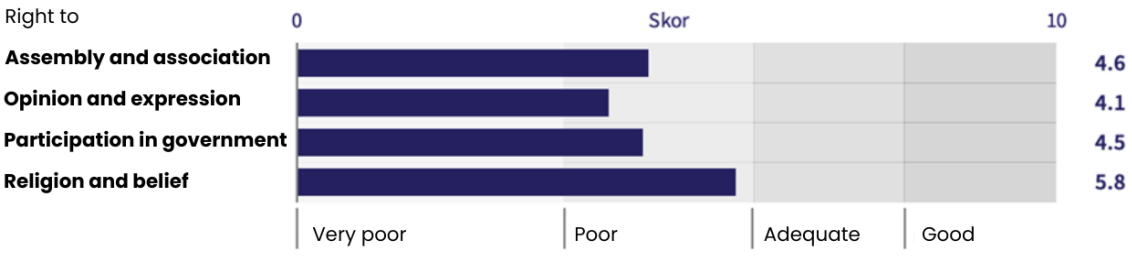
[42] Amnesty International, "A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia."

[43] Fabio Angiolillo, Ana Good God, and Staffan I. Lindberg, "DEMOCRACY REPORT 2025: 25 Years of Autocratization – Democracy Trumped?" (V-Dem Institute, March 2025).

[44] The downward trend in the democracy index is evident in The Economist Intelligence Unit's 2025 report. Indonesia's democracy index in 2024 declined again compared to 2023, leaving it still in the flawed democracy category. Of the five dimensions measured, the lowest scores were in the realm of political culture and civil liberties. According to The Economist Intelligence Unit's (EIU) 2025 report on the 2024 Democracy Index, Indonesia's Democracy Index reached a score of 6.44 on a scale of 10. This achievement places Indonesia in 59th place out of 167 countries measured by the index. With this score, Indonesia is also in the flawed democracy category. Indonesia's position in the flawed democracy category is not new, but has occurred over the past decade. This indicates a continuing downward trend in Indonesia's Democracy Index score.
See Nino Citra Anugrahanto and Kurnia Yunita, "One Decade of Declining Trend in Indonesia's Democracy Index," *Kompas.id,* 5 March 2025, https://www.kompas.id/artikel/satu-dekade-tren-indeks-demokrasi-indonesia-menurun . Accessed on 9 January 2026.



The poor human rights situation can be seen in the assessment results of the Human Rights Measurement Initiative (HRMI). Indonesia's Empowerment Score of 4.4 out of 10 indicates that many people in Indonesia cannot enjoy their civil rights and political freedoms, including freedom of speech, assembly and association, and democratic rights. In this context, when compared to other countries, Indonesia's performance is worse than average in terms of empowerment rights. Indonesia's empowerment score according to the Human Rights Measurement Initiative (HRMI) can be seen in the following diagram.[45]



[45] Human Rights Measurement Initiative (HRMI), "Indonesia: Rights Tracker," *RightsTracker.org,* https://rightstracker.org/country/IDN . Accessed on 9 January 2026

Reflecting on the repressive and terrorizing actions taken against the public who vocally criticize various bad government policies, in 2026 public criticism will be met with repressive actions that are predicted to become even stronger.[46] Furthermore, this study aims to examine how the Government of the Republic of Indonesia responds to the use of spyware devices through the development of a policy ecosystem, specifically the procurement of spyware devices supported by public funds. Public procurement should be an instrument to address human rights risks in the use of digital technology, including spyware devices. The use of public funds in the procurement of spyware technology has legal implications that lead to public accountability for the procurement of such technology because public funds are derived from taxes charged to the public. Accountability is the responsibility of all actors involved in the procurement of spyware technology and is an important path for victim recovery to hold accountable those who cause human rights violations.

B. Research Questions

Based on the background description above, this research starts from several problem formulations, as follows:

1. What is the spyware usage ecosystem in Indonesia?
2. What are the human rights impacts of spyware use in Indonesia?
3. How is the relationship between the state and the private sector in the use of spyware in the landscape of business and human rights norms in regulating the commercialization of spyware?
4. What is the mechanism of accountability of spyware technology use by state officials because the procurement of this technology is supported by public funds?

[46] Bagja Hidayat, "Indonesia 2026: Increasingly Noisy, Increasingly Repressive," *Tempo,* January 4, 2026, https://www.tempo.co/prelude/sampul-tempo-edisi-khusus-indonesia-2026-2104222 . Accessed on 8 January 2026.

C. Research Methods

This study uses Amnesty International's research titled *A Web of Surveillance: Unraveling A Murky Network of Spyware Exports to Indonesia* as a reference. However, this study attempts to raise another dimension that has not been further elaborated by Amnesty International, namely public procurement, spyware technology is examined through a public budget perspective based on a human rights budgeting approach. The literature research stage took place from September 2025 to December 2025. Initial findings based on this literature research were validated through a series of focus group discussions with academics, researchers, and civil society organizations focusing on technology and human rights issues, security sector reform, and budget transparency.

Therefore, this study is based on library research on the intersection between the use and exploitation of spyware and its impact on human rights. Furthermore, this study includes non-academic sources by referring to similar thematic reports, news coverage of spyware, and other sources. To deepen this picture, this study also refers to interdisciplinary academic literature considering the dynamic nature of spyware commercialization. Budget analysis is one of the units of analysis for spyware purchases because, from a human rights perspective, public procurement of goods or services should consider and address human rights risks and strengthen essential public services. Public budget analysis can be used to examine the extent to which public procurement policymakers, purchasers, and contract managers are committed to and aligned with human rights risks and considerations. The provision of essential public services is a way for the State to fulfill its human rights obligations.[47] In relation to the use of public funds, the use of spyware should not be aimed at spying on citizens, especially those critical of state policies.

It is crucial for the tax system to consider a human rights perspective and a human rights-based approach to make the tax system more progressive,

[47] Daniel Morris and Cathrine Bloch Veiberg, "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to Deliver Essential Public Services" (Copenhagen K: The Danish Institute for Human Rights, February 2024).

transparent, and equitable, with the aim of combating inequality, addressing climate change, financing public services equitably, promoting inclusive economic growth, and preventing abuse of power. The UN Special Rapporteur on extreme poverty emphasized the importance of designing public policies, including tax policies, with a human rights approach.[48] Therefore, tax revenues will impact rights because taxes are the primary source of revenue for providing health and education services, access to public transportation, financing a well-functioning judicial system, and effective legal and government administration.[49] This means that taxes have the potential to strengthen civil and political rights. When individuals contribute to state revenue by paying taxes, the allocation and spending of these resources should encourage the right to participate in politics and strengthen the social contract between citizens and the state. A further logical consequence is encouraging greater government accountability, transparency, and responsiveness in allocating and spending resources for the public good (*bonum commune*).[50] Thus, fiscal policy has a direct impact on rights. For example, a country may have a policy of financing budget allocations that endanger citizens' rights. Likewise, the state must ensure that conditions exist so that third parties do not violate rights through the provision of goods and services that are not intended to reduce the enjoyment of citizens' rights.[51]

However, efforts to identify the misuse of commercial spyware technology through policy analysis have proven to be a complex and challenging issue due to the lack of transparency in the procurement of such devices. This lack of transparency in spyware procurement stems from limited market data and the actors involved in the spyware supply chain, including the tracking of budget

[48] Rodrigo Uprimny Yepes and Mariana Matamoros, "A Human Rights-based Approach to Tax Systems," *Dejusticia,* October 2024, https://www.dejusticia.org/en/a-human-rights-based-approach-to-tax-systems/ . Accessed on 9 January 2026.

[49] "Inequalities and Democracy and Human Rights," *Tax Justice Network,* 13 November 2020, https://taxjustice.net/topics/inequalities-and-democracy-and-human-rights/ . Accessed on 9 January 2026

[50] Alexandra Hever, "The Price of Inequality: Why Tax Is a Human Rights Issue," *HRRC,* 27 June 2025, https://www.humanrightsresearch.org/post/the-price-of-inequality-why-tax-is-a-human-rights-issue . Accessed on 9 January 2026.

[51] The Initiative for Human Rights Principles in Fiscal Policy, *Principles for Human Rights in Fiscal Policy,* May 2021.

allocations scattered across ministry/institutional spending. In this context, given the secrecy surrounding spyware use and the challenges of conducting research on this topic, this study is exploratory in nature, rather than an attempt to provide a comprehensive or definitive analysis and review of spyware and its threats to human rights and accountability for commercial spyware use in Indonesia. Consequently, any information presented in this study is more of an indication of trends and potential developments, requiring further research to organize this initial information. Further research on spyware use in Indonesia is essential for organizing this scattered information to create a more complete picture of spyware use and its impact on human rights and accountability for commercial spyware use in Indonesia.

Based on the description above, the research method used in this study can be described in the image below.



D. Device Characteristics, Spyware Operations, and Types of Threats to Targets

Spyware provides complete and unrestricted access to every device, leaving the target unaware of its existence. Those operating the spyware can now read every email and text message sent and received, even if encrypted. The technology can scan the camera roll for incriminating personal photos for potential blackmail and track the phone's movements by reading the Global

Positioning System (GPS). It can also secretly activate the camera and microphone, turning the device into a real-time wiretap. At the same time, it can activate a self-destruct feature and erase all traces of the fake WhatsApp call. In a crime scene analogy, this technology can sweep the crime scene to remove fingerprints. It's as if an invisible spy has slipped undetected into the target's pocket and is seeing the world through their eyes, with the target unaware their phone has been hacked.[52]

Meanwhile, there are approximately 7.64 billion people, and nearly three-quarters of them own at least one personal mobile phone. Regardless of the brand of personal phone used, these pocket devices serve as electronic portals to the outside world. These personal phones scattered around the world are potentially selected as targets via the internet, radio waves, and ethernet cables, traveling at near-light speed in near-total silence. A special message containing complex instructions is sent to each target device disguised as a video call on the popular communication app WhatsApp. The instructions exploit a security flaw in the app's code that escapes even the most trained WhatsApp technicians. These instructions trigger a buffer overflow, a digital short circuit that disrupts the app's memory processing system, temporarily interrupting it and leaving it open to further attacks. The ultimate goal is to break the system's lock and leave a gaping hole, allowing a more complex program to slip in undetected.[53]

Spyware is software designed to collect data or spy on user activity without permission and then transmit it to a third party without the user's consent.[54] Elaine Korzak defines spyware by adding the element of surveillance or data collection purposes, as follows:[55]

---

[52] Global Justice Clinic, "Attempted Digital Surveillance as a Complete Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights."

[53] Ronald J. Deibert, *Chasing Shadows: Cyber Espionage, Subversion, and the Global Fight for Democracy* (Toronto: Simon & Schuster, 2025).

[54] "What Is Spyware? Definition, Types and Protection," Fortinet, nd, https://www.fortinet.com/resources/cyberglossary/spyware .

[55] Differences in individual or institutional preferences then give rise to a variety of other terms frequently used in international debates, including cyber surveillance technology, hackers-for-hire, cyber mercenaries, or, more recently, "commercial cyber intrusion capabilities." Definitions of all these terms vary among various

"Software that facilitates unauthorized remote access to internet-connected devices for the purposes of surveillance or data collection."

Meanwhile, Giovanni Sartor and Andrea Loreggia describe spyware through its various operational dimensions as follows:[56]

1) Spyware designed to collect information about a user without the user's knowledge or consent;
2) Spyware can track users' online activities, steal personal information, or display unwanted advertisements;
3) Spyware can spread through infected files or emails, or it can be bundled with other software and installed without the user's knowledge;
4) Spyware can also download other malicious programs from the internet and install them on the device.

Complementing the previous perspective, Mike Sexton dissects the characteristics of spyware, placing particular emphasis on the commercial dimension and third-party involvement. According to Sexton, the main characteristics of spyware include:[57]

1) Commercial malicious software;
2) Installed on a computer or mobile device without the user's consent or knowledge;
3) Hacking, surveilling, and collecting data secretly from a distance; and

governmental and non-governmental stakeholders. See Elaine Korzak, "Managing Commercial Spyware Through Export Controls: Lessons Learned from the Wassenaar Experience" (Center for Long-Term Cybersecurity (CLTC) UC Berkeley, March 2025).

[56] Giovanni Sartor and Andrea Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes" (European Union, 2022).

[57] Mike Sexton, "What Is Spyware and Why Should Policymakers Care?," *Third Way,* 9 March 2023, https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care . Accessed on 16 December 2025.

4) Forwarding such data to third parties.

Based on these characteristics, an operator can perform secret data collection remotely on infected devices, including mobile phones and computers.[58] Spyware is a technology that facilitates remote infiltration into personal computers, smartphones, and other electronic devices, and results in the exfiltration or planting of data, or the use of device features, such as microphones, cameras, messages, and others to gather additional information about the owner or his acquaintances, without their knowledge.[59]

The sophistication of various types of spyware is determined by two parameters: (1) how the spyware infects the device; and (2) the spyware's ability to collect or retrieve information from the device. A common, less sophisticated example of a spyware infection is when a user clicks on a pop-up window link, or opens an email attachment from an unknown source, and the computer shuts down or restarts. This disruption in computer function can signal to the user that the computer being used has just been infected with malware. Some forms of spyware only perform a single function, such as tracking the device's location or keystrokes on the computer. At the top of the spyware hierarchy is Pegasus,[60] which has the ability to unlock and transmit the entire contents of a mobile device, in addition to taking control of the device's microphone and camera, without requiring user input.[61]

Furthermore, when considering vulnerability analysis and exploitation of

[58] Julie Bloch et al., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent," *Just Security,* 15 May 2019, https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/ . Accessed on 16 December 2025.

[59] Tamar Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, 3 April 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661

[60] Pegasus spyware can infect users' devices using *zero-click vulnerabilities,* which are vulnerabilities that require no user interaction or intervention. In the past, *spyware* required users to open an infected file or click a malicious link to access a device. By exploiting *zero-click vulnerabilities,* malware can infect a device simply by exploiting weaknesses in the operating system, software, or network connection. Because users are unaware of the infection, it is more difficult to recognize and protect against such attacks. See Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

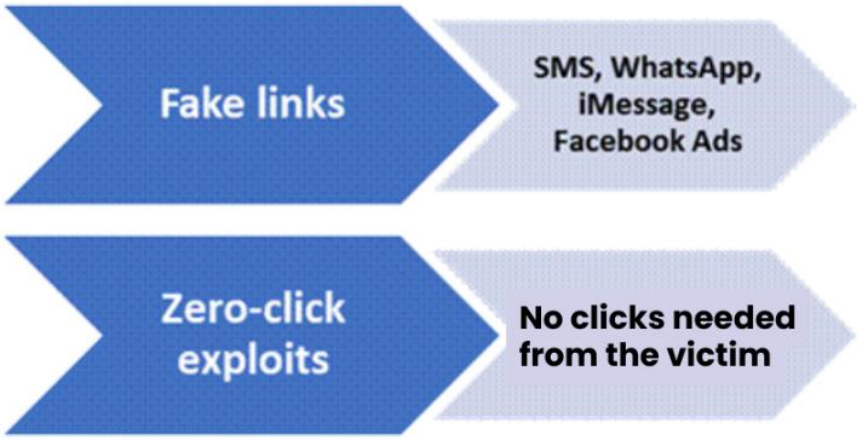
[61] Katherine Kuhl, "Pegasus Spyware in Hungary: Analyzing Hungary's use of Pegasus on journalists with Lessig's Four Modalities of Regulation" (Senior Theses, Fordham University, 2024).

targeted victims there are two different types of attacks:[62]

1) Zero-click attacks require no user intervention. These attacks are often based on zero-day vulnerabilities and are particularly dangerous because users are often unaware of the attack and therefore unable to counter it or mitigate its impact.

2) One-click attacks require an action from the targeted user, typically clicking a link or button displayed within a web application. The victim, while required to perform the action, may be unaware of the attack due to being misled by the attacker's misleading message or interface.

The operating method of spyware devices is divided into two as shown in the image below.[63]



Spyware have been circulating on the internet since the mid-1990s, and government security and intelligence agencies have allegedly been producing and deploying software to intercept digital communications for years. Later, spyware were also produced and marketed by commercial companies. The software they produce have become increasingly sophisticated and invasive. Today, some spyware devices allow for real-time and remote capture of audio and visual input and communications, allowing the operator of the infected

[62] Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."
[63] Image of the results of data processing carried out by FITRA

device to spy on the target and those around them. Companies such as NSO Group in Israel, Finfisher in the UK and Germany, and Hacking Team in Italy are key players in this rapidly growing and secretive industry. In 2019, NSO sold Pegasus for $1 billion, and Moody's estimates the spyware industry as a staggering $12 billion market.[64]

The proliferation and misuse of commercial spyware technology now poses serious challenges to international policy. The rapidly expanding spyware market now provides a variety of technologies capable of covertly accessing and/or monitoring the communications data of individuals and groups. Governments and non-governmental stakeholders worldwide have been working to address the human rights violations and national security risks associated with the misuse of commercial spyware technology.[65] The use of spyware poses a unique threat because it is more intrusive than other instruments of digital repression and difficult, if not impossible, to block. Spyware operates covertly and often leaves no trace, facilitating law enforcement efforts. These tools are also easier for governments to use than conventional methods of repression and coercion, as well as some more technologically sophisticated passive surveillance systems.[66]

One of the most notorious surveillance tools is Pegasus, a spyware suite developed by the Israeli company NSO Group.[67] While marketed as a tool to combat terrorism and crime, empirical evidence suggests it has become a weapon for authoritarian governments to target journalists, activists, political opposition figures, and marginalized communities. Its ability to infect devices without user interaction (zero click) has made it an unprecedented surveillance tool. This provides states with an opportunity to suppress opposition while

[64] Bloch et al., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent."
[65] Bloch et al., "CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent."
[66] Gail Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa" (Master's thesis, Harvard University, 2023).
[67] NSO Group was founded in 2010 by Israeli entrepreneurs Niv Carmi, Shalev Hulio, and Omri Lavie. NSO Group licenses surveillance products to intelligence and law enforcement agencies worldwide. The company is particularly known for its Pegasus *spyware,* an invasive malware capable of covertly taking control of smartphones and remotely extracting their contents. See Dan M. Kotliar and Elinor Carmi, "Keeping Pegasus on the Wing: Legitimizing Cyber Espionage," *Information, Communication & Society* 27, no. 8 (2024): 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873 .

avoiding accountability. The widespread and unchecked deployment of Pegasus has exposed the gap between global digital security and the lack of regulatory oversight governing the sale and use of this surveillance tool. In the context of conflict zones, such as Palestine[68] and Kashmir, the use and exploitation of Pegasus spyware demonstrates the growing interconnectedness between state surveillance, corporate interests, and digital authoritarianism.[69]

By exploiting zero-day vulnerabilities, Pegasus can infiltrate devices automatically without any clicks. A zero-day vulnerability is a vulnerability in software that has not yet been identified or patched by the software developer. The software developer does not have even one day to respond to or fix the issue. By exploiting these undisclosed vulnerabilities, the spyware can evade detection and gain unauthorized access to a device or network.[70]

Pegasus is a spyware tool capable of accessing and hacking mobile phones, turning them into listening devices without the user's knowledge. These hacking attempts rely on users installing malware or unknowingly clicking on fake links to gain access. Once access is gained, Pegasus can read text messages, track calls, collect passwords, track location, access the device's microphone and camera, and gather information from apps. This spyware can access a user's phone through system vulnerabilities, such as email and various apps, such as Apple Music and iMessage, allowing the spyware to track all forms of

[68] Israel has embarked on a genocidal campaign against Palestinians by deploying various surveillance systems, including drones, communications interception systems, facial recognition technology, and artificial intelligence targeting systems, including Gospel, Lavender, and Where's Daddy. Furthermore, Israel's Unit 8200 has developed a Large Language Model (LLM) to analyze intercepted communications from Palestinians and likely feed this information to other systems. These systems utilize mass surveillance information on Palestinians in Gaza and identify suspects for targeting. These systems are even deliberately used to target suspects while they are in their homes, and without regard for proximity to civilians and civilian infrastructure. Israel has expanded its surveillance and interception practices across the internet, social media, phones, messaging apps, and other digital platforms. In this context, Israel has deployed spyware, most notably Pegasus from the NSO Group. See, Mais Qandeel and Özgün Erdener Topak, "Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis," *Journal of Genocide Research* (October 2025): 1-22, https://doi.org/10.1080/14623528.2025.2567372 .

[69] Samia Afrose, "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine" (Bachelors thesis, Harvard University, 2025).

[70] Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

communication and location through the phone's camera and microphone.[71] Pegasus software infects iPhones and Android devices, allowing operators to extract messages, photos, and emails, record calls, and secretly activate the microphone and camera.[72] How the Pegasus tool works to target users can be seen in the image below.[73]



[71] The use of surveillance technology to infiltrate personal devices is nothing new. Edward Snowden's revelations in the 2010s revealed the National Security Agency's (NSA) ability to remotely activate mobile devices, including accessing their microphones and cameras, even when they are turned off. As long as the battery is still in the device, personal devices are at risk of surveillance. This is part of the NSA's mass surveillance program, which allows the United States government to collect Americans' communications data, metadata, and content without warrants, and store their information in data centers and repositories. See Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

[72] "Pegasus: Spyware Sold to Governments 'Targeted Activists'," *BBC News,* 19 July 2021, https://www.bbc.com/news/world-57891506 , Accessed on 6 January 2026.

[73] "Pegasus: Who Are the Alleged Victims of Spyware Targeting?"

In the case of Jamal Khashoggi, if his phone or the phone of a family member were hacked by Pegasus, conversations, location, and other sensitive information could be intercepted and accessed. This information interception played a crucial role in the planning and execution of Jamal Khashoggi's murder. Pegasus's extensive capabilities allow the software to exploit phone functions, violating the privacy of the targeted individual and the privacy of individuals associated with the target.[74]

Several cases demonstrate that the evolution of Pegasus spyware lies in the sophistication of its infection methods and the scale of its spread. Its key innovation is its ability to operate without requiring any user interaction and to bypass some of the most sophisticated security measures. This contrasts with National Security Agency (NSA) operations, which generally rely on network-based interception or malware installation that requires a certain degree of user negligence. Meanwhile, Pegasus' use is no longer limited to state intelligence agencies. The technology is sold commercially to governments worldwide, ultimately fueling the creation of a global digital repression market.[75]

Spyware with characteristics like Pegasus, which has the powerful ability to access all connected devices and data, indiscriminately and without restrictions, violates the basic standards of necessity and proportionality under international human rights law. According to David Kaye, the nature of current spyware demands that we go beyond a mere moratorium, namely by seeking a complete ban on this invasive technology, whether provided by the private or public sector. Given the serious threat these devices pose to human rights, no government or private company should be permitted to sell similar technology to any party.[76]

---

[74] Ottavio Marzocchi and Martina Mazzini, Pegasus and surveillance spyware, Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, 2022.
[75] "Pegasus: Who Are the Alleged Victims of Spyware Targeting?"
[76] David Kaye, "David Kaye: Here'S What World Leaders Must Do About Spyware," Committee to Protect Journalists, 12 October 2022, https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/#:~:text=Read%20CPJ%20's%20complete%20special%20report,to%20hack%20into%20individual%20phones. Accessed on 2 January 2026

The technical capabilities offered by commercial spyware have attracted the attention of many countries. The United States, for example, is listed as one of the governments considering using technology from vendors like the NSO Group and other companies. According to media reports, Pegasus allows operators to remotely and covertly install software on a user's mobile phone or other digital device that can secretly access user data and monitor all of their activities. Pegasus does more than simply track metadata, such as usage statistics or call logs; it provides access to all data contained on the phone, monitoring GPS, real-time audio and visual recording via camera and microphone, and many other capabilities. The latest version of Pegasus reportedly no longer requires action from the target to click on links (zero-click). Pegasus allows operators to infect phones simply by using the target's phone number. New evidence has emerged confirming this capability: exploiting a security flaw in the WhatsApp messaging service, NSO's spyware can secretly install surveillance software simply by placing a call to a target's phone, even if the target doesn't pick up. Because Pegasus installation leaves no trace detectable by ordinary users, finding evidence of its infection requires digital forensics by trained tech experts, such as those at Citizen Lab and Amnesty International.[77]

Digital surveillance technologies, including spyware, are known as dual-use goods, meaning they can be used for both defense and civilian purposes. Dual-use technologies in 42 countries fall under the multilateral export control regime of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies of 1996. In 2013, the Wassenaar Agreement was amended to include intrusion software. Although the Wassenaar Agreement is not legally binding, signatories typically voluntarily adopt the control list into domestic regulations. This requires companies whose products are listed to obtain special licenses before exporting those goods.[78]

---

[77] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*

[78] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

E. Spyware and the Interests of State Power: Spyware Operations in Various Countries

Although marketed as neutral instruments for use by law enforcement or in national security, spyware, facial recognition tools, and biometric systems have been allegedly used to facilitate human rights violations. Surveillance technology has arguably become a crucial instrument of state power, particularly in the context of control by authoritarian regimes. At the same time, the use of surveillance has allegedly enabled transnational repression. Dissidents living in exile have allegedly been monitored, harassed, and even kidnapped or killed with the aid of digital tracking devices. These developments raise serious legal and ethical concerns, particularly when private companies provide technology that is then implicated in political repression, illegal surveillance, or the targeting of dissidents.[79] These devices often have dual uses, meaning they have legitimate applications in criminal investigations or for national security purposes, but can be repurposed to suppress dissent or target minority groups.

There are several reasons why a third party might be interested in gaining unauthorized access to a device or group of devices:[80]

A. Collecting information about the target (device user), including personal data, such as name, address, and telephone number, as well as information about the target's online activities and habits;

B. Collecting information about the target's acquaintances, including data about the people the target communicates with, as well as information about their online activities and habits;

C. Gaining access to a device for the purpose of demanding ransom. In

[79] Vladimir Hrle, "Corporate Responsibility in the Age of Surveillance and Transnational Repression: Legal Obligations and Human Rights Due Diligence," *International Bar Association,* 21 August 2025, https://www.ibanet.org/corporate-responsibility-in-age-of-surveillance-and-transnational-repression-legal-obligations-human-rights-due-diligence. Accessed on 11 January 2026.

[80] Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

this case, a third party may attempt to take control of the device and make its contents inaccessible by encrypting it, then demanding payment in exchange for returning control of the device to the user and allowing access to the data.

D. Identity theft: If a third party gains access to a device, they can impersonate the device's owner and send messages or perform other actions that appear to originate from the legitimate owner. This can be especially dangerous if the third party can access sensitive personal or financial information through the device.

E. Making the target unable to use the device. This can be done by deleting important files or disabling the device's core functions.

The PEGA Committee report summarizes the human rights risks associated with the unregulated commercial spyware market as follows:[81]

"The misuse of spyware not only violates individuals' privacy rights. It insidiously undermines democracy and democratic institutions. It silences opposition and critics, eliminates oversight, and has a chilling effect on the free press and civil society. It also serves to manipulate elections. The term 'mercenary spyware' perfectly reflects the nature of this product and industry. Even a failed attempt to infect a smartphone with spyware has political consequences, and can harm both individuals and democracy. Participation in public life becomes impossible without the assurance of freedom and unobservance."

The use and deployment of spyware as part of surveillance is often motivated by power. The term "surveillance" itself is French for "watching from above." Surveillance efforts imply power relations. This is not simply passive surveillance, but rather a form of surveillance that assesses and intervenes to shape behavior. The goal of surveillance is to ensure that individuals are unaware of these control dynamics to be effective. These dynamics are more effective

[81] Costica Dumbrava, *Impact of the Use of Spyware on Fundamental Rights* (Brussels: European Parliamentary Research Service,2023), https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf

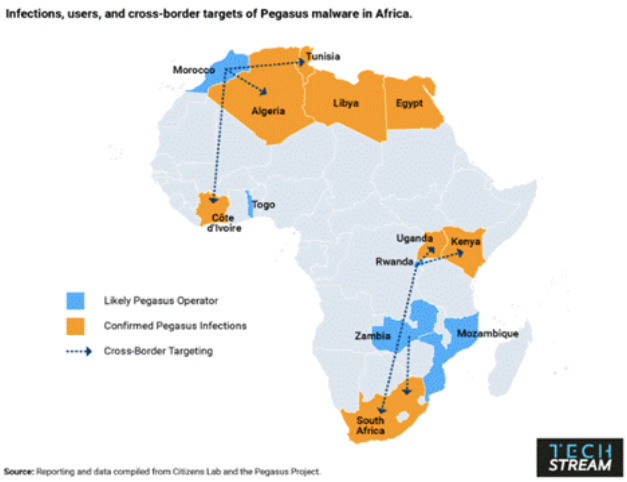
when they are perceived as normal, with the underlying political content obscured. In other words, surveillance is understood as the monitoring of individuals in order to dictate or control their behavior.[82]

Spyware is frequently misused in many countries. Its use has serious implications for privacy, data security, and public trust. There are currently 11 types of spyware worldwide, each with varying levels of capability.[83] Human rights activists, journalists, and lawyers worldwide have been targeted by authoritarian governments using spyware software sold by the Israeli surveillance firm NSO Group. The Pegasus Project revealed the identities of individuals whose names appeared on the target list, including hundreds of business executives, religious figures, academics, activists, union officials, and government officials, including cabinet ministers, presidents, and prime ministers.[84] The Pegasus Project successfully identified targeting patterns by individual clients through leaked data and identified 10 governments believed to be responsible for the selection of targets: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates.[85]

In Africa, the widespread use of NSO Group's Pegasus spyware has been confirmed. Rwanda and Morocco have been identified as the primary operators, with Morocco being the region's largest client. Pegasus spyware has exacerbated political tensions in African countries because, in addition to being used to spy on terrorists and criminals, it has also been used to spy on political opponents, human rights activists, and civilians. Pegasus applications in Africa have targeted up to 10,000 phone numbers, including that of King Mohammed VI himself. Zambia is also suspected of using this technology to spy on political opponents

[82] Torin Monahan and David Murakami Wood, "Introduction: Surveillance Studies as a Transdisciplinary Endeavor," in *Surveillance Studies: A Reader,* ed. Torin Monahan and David Murakami Wood (Oxford: Oxford University Press, 2018).
[83] See appendix I of this study.
[84] Stephanie Kirchgaessner et al., "Revealed: Leak Uncovers Global Abuse of Cyber-surveillance Weapon," *The Guardian,* 18 July 2021, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus . Accessed on 7 January 2026.
[85] Kirchgaessner et al., "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapons."

during the administration of former President Edgar Lungu.[86] The spread of Pegasus in Africa, including the countries operating it[87] and those infected, can be seen in the map below.[88]



Meanwhile, in the ASEAN region, pro-democracy activists in Thailand also faced the Pegasus spyware. This application targeted pro-democracy activists and monarchy reformers in Thailand. At least 30 individuals, including protesters, lawyers, and pro-democracy activists, were infected with Pegasus between October 2020 and November 2021. The infection was carried out through a zero-click exploit, allowing hacking without the victim's knowledge, granting access to phone data such as messages, location, and camera or microphone recordings. The Citizen Lab, iLaw, and DigitalReach found evidence of spyware attacks on the pro-democracy movement, with indications that several Thai government agencies may have been involved, including those linked to other NSO products like Circles.[89]

---

[86] https://www.brookings.edu/articles/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/

[87] "Likely Pegasus Operator" refers to the five African countries identified either by Citizens Lab or Pegasus Project reporting as a country that licenses or operates Pegasus malware. Pegasus infections have been found in all countries that are suspected operators except for Mozambique. By contrast, there were confirmed infections in eight African countries who are not suspected of being operators.

[88] This map references www.brookings.edu

[89] John Scott-Railton et al., "GeckoSpy: Pegasus Spyware Used Against Thailand's Pro-Democracy Movement - the Citizen Lab," The Citizen Lab, 7 July 2022, https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/ .

The use of Pegasus spyware by authorities has been confirmed, among other things, in the murder of Saudi journalist Jamal Khashoggi. Khashoggi's phone was hacked and spied on while he was visiting the Saudi Consulate General in Istanbul. Agnes Callamard, Special Rapporteur regarding extrajudicial killings concluded that:[90]

"The execution of Jamal Khashoggi is the most glaring example of a different pattern: the threat or use of extraterritorial force by one state against individuals in another state's territory, outside of situations of armed conflict, by one state against individuals in another state's territory. This execution resulted in human rights violations, including extrajudicial killings, abductions, and forced surrenders that can result in torture, imprisonment, enforced disappearance, and death. Other resulting violations can also include violations of freedom of expression or the right to privacy. Fleeing abroad in search of safety is increasingly unreliable as a form of protection."

The Special Rapporteur's report references Citizen Labs' analysis of the infiltration of Jamal Khashoggi and his associates by Pegasus operatives linked to Saudi Arabia. Pegasus, the NSO spyware suite, allows Saudi-linked operatives to access phone contacts, photos, text messages, online chat logs, emails, and other private files.[91] Intelligence infrastructure and surveillance technology are particularly dangerous weapons in the hands of autocratic and internationally sanctioned states, such as Venezuela and Saudi Arabia, which have used such technology to target civilians, journalists, dissidents, and ethnic minorities.[92]

Mass surveillance treads a fine line between protecting citizens and violating their privacy. Data collected in mass surveillance disregards

[90] UN Human Rights Council, *Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi,* A/HRC/41/CRP.1 (19 June 2019).
[91] UN Human Rights Council, *Investigation into the Unlawful Death of Mr. Jamal Khashoggi*.
[92] Ronnie Rosen Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading," *Georgetown Law,* 30 January 2023, https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/ . Accessed on 20 January 2026.

international borders, and cross-border data collection impinges on a number of rights protected by privacy protections, including the rights to freedom of expression, freedom of conscience and religion, freedom of assembly, freedom of association, and other rights.[93] Despite the intrusive nature of these tools and their potential threat to human rights, companies from countries such as France, Germany, and Italy have sold invasive technology to regimes like the Syrian government. Hacking Team emails published by WikiLeaks in 2015 revealed that an Italian company sold its invasive tools to Ethiopia, Nigeria, South Sudan, Bahrain, Uzbekistan, Azerbaijan, Kazakhstan, Russia, Saudi Arabia, and many other governments with authoritarian or single-party systems.[94] The table below lists countries using Pegasus and Predator spyware as follows:[95]

Spyware	User Country
Pegasus	Israel (Developer), Mexico, Saudi Arabia, UAE, India, Azerbaijan, Morocco, Rwanda, Togo, Hungary, Poland, Spain, Thailand, Indonesia (alleged), Kazakhstan, Uzbekistan, Vietnam, Egypt, Bahrain, Oman, USA, Jordan, Pakistan (alleged), Singapore (alleged client state), Lebanon.
Predator	UAE, Morocco, Indonesia (alleged), Türkiye, Greece, Cyprus, Italy, USA.

While some governments may produce their own devices for targeted digital surveillance, many countries purchase the advanced technology enabling such surveillance from private companies. States often justify the procurement

[93] Anna W. Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware," *The Brooklyn Journal of International Law* 44, no. 2 (7 January 2019).
[94] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."
[95] Data processed by FITRA

of this technology by arguing that it is necessary to maintain law and order. Some of these surveillance companies produce and sell spyware or other similar tools to states. Beyond legitimate purposes, these devices are used as surveillance instruments, narrowing the space for dissent by targeting human rights defenders. Such targeted digital surveillance attacks involve the interaction of multiple state and non-state actors, including private companies, investors, law enforcement and intelligence agencies, national export control authorities, and multilateral export control regimes such as those embodied in the Wassenaar Agreement and the European Dual Use Regulation.[96] Regulatory gaps, abuse by state agents, and state and corporate secrecy contribute to the obstacles and complexities involved in identifying, preventing, or seeking redress for human rights violations caused by these attacks, including establishing adequate oversight mechanisms.[97]

The security risks posed by the proliferation of commercial spyware have become a key foundation for reforming the policy ecosystem to prevent the misuse of such surveillance technologies. The United States has taken two significant cybersecurity measures since 2019: (1) Section 889 of the John S. McCain National Defense Authorization Act of 2019 (NDAA 2019); and (2) the Cybersecurity Maturity Model Certificate. The first measure seeks to protect cybersecurity in the defense industrial base by severely restricting the ability of both federal agencies and federal contractors to use supplies or services from Huawei Technologies Company (Huawei), Zhongxing Telecommunications Equipment Corporation (ZTE), and three other Chinese companies that provide surveillance and telecommunications hardware and services. While a measure aimed at ensuring cybersecurity, Section 889 seeks to ensure procurement supply chains by ensuring that procurement supply chains are located in the domestic market or reliable allied markets. In contrast, under the Cybersecurity Maturity Model, the Department of Defense pursues cybersecurity through a

[96] Amnesty International, Privacy International, and The Center for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."
[97] Amnesty International, Privacy International, and The Center for Research on Multinational Corporations (SOMO), "Operating From the Shadows: Inside NSO Group's Corporate Structure."

comprehensive set of cybersecurity practices that contractors on a defense industrial basis must follow when handling Federal contract information and Controlled Unclassified Information (CUI).[98]

The increasing use of commercial spyware is not only a problem in the United States, but also in the European Union. Following the 2021 disclosure of Project Pegasus, which showed that the Pegasus hacking toolkit was used to spy on journalists, politicians, activists, and others worldwide by clients of the Israeli firm NSO Group, the European Parliament established a committee of inquiry (PEGA Committee) to further investigate the use of commercial spyware in the EU. The European Parliament adopted recommendations calling on the European Commission to more strictly regulate the use, manufacture, and trade of spyware; to more stringently enforce existing laws; and to establish a clear definition of national security.[99]

At this point, the characteristics of the intersection between government and private interests complicate efforts to regulate the use of commercial spyware due to the following obstacles:[100]

First, the policy ecosystem, including legislation, regulations, and budgeting, is characterized by a high degree of opacity. Most companies operating in this sector are not widely known or publicly disclosed, resulting in limited publicly available information about the business. The minimal transparency of the commercial spyware market impacts all elements of the supply chain: vendors, buyers, users, and decisions regarding licensing, transfer, and export.

Second, governments play a central role in all aspects of the commercial spyware technology product lifecycle, thus having critical implications for the

[98] Stuart Joseph Anderson, "Comparing Section 889's Huawei Ban and the Cybersecurity Maturity Model Certificate: The Challenge of Pursuing Cybersecurity Through Friend-Shoring," *Public Contract Law Journal* 54, no. 2 (2025).
[99] Sophie in 't Veld, "An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?," Digital Front Lines, nd, https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/ . Accessed on 7 January 2026.
[100] Korzak, "Managing Commercial Spyware Through Export Controls: Lessons Learned from the Wassenaar Experience."

policy ecosystem itself. Furthermore, governments are not merely buyers and users of commercial spyware technology. Rather, they are key actors at all stages of the commercial spyware product lifecycle. Governments represent the interests of the countries of origin of the spyware companies that develop and manufacture these technologies, and they wield significant power to shape the business and investment environment. At the same time, countries are also regulatory authorities, responsible for regulating their own governments' behavior and use of spyware technology, as well as granting or denying export licenses to companies seeking to sell this technology to foreign entities. The key role of governments in the commercial spyware market, coupled with their conflicting roles as users and regulators, creates tensions that create challenges for establishing national and international restrictions on commercial spyware.

Third, commercial spyware technology meets the needs of states to acquire capabilities that allow them to remotely access and manipulate digital devices, systems, or networks without authorization. To mitigate the risks, states emphasize that these tools and services must be developed and used only for lawful purposes through the implementation of a Code of Conduct. The Pall Mall Process Declaration specifically states that the use of such technology must remain within the legal framework, such as for national security and defense, the investigation and prevention of serious crimes, and cybersecurity activities.

Digital technologies, including spyware, are generally designed by the private sector to meet specific government orders and needs. The use of Pegasus by several state institutions in Indonesia highlights the existence of a state-private nexus, which has direct implications for human rights protection obligations. These contractual relationships often create accountability gaps, where the secrecy of procurement contracts and the complexity of the technology are often used to obscure responsibility for the resulting intrusive impacts.

In practice, public authorities and private providers often collaborate to tailor technology features to specific operational needs. This situation

emphasizes the state's obligation to ensure that technology acquired through public procurement does not harm rights holders. The United Nations Guiding Principles (UNGPs) emphasize that commercial transactions between states and companies provide unique leverage. Through the terms of procurement contracts, states have a bargaining position to improve standards of respect for human rights by those companies. Thus, procurement is not simply a business transaction, but a legal instrument for states to prevent the misuse of surveillance technology.[101]

The UN Special Rapporteur on the Right to Freedom of Opinion and Expression articulates the close collaboration of governments and the private sector in the digital surveillance market. However, the entire spectrum of this collaboration, from due diligence and sales to technical support for end users, generally operates under very limited oversight and transparency. In this regard, Citizen Lab identified the existence of a vulnerability market exploited collectively by governments and private actors. This market serves as a space for exploiting zero-day vulnerabilities to gain illicit access to individuals' private communications and devices in a clandestine manner.[102] The proliferation and misuse of surveillance technology is a major concern for the UN Special Rapporteur on the Promotion and Protection of Human Rights in the Context of Counter-Terrorism. This is due to the significant risks to fundamental rights arising from overly broad and ambiguous definitions of counter-terrorism and security objectives. This lack of clarity often serves as an excuse for both states and private actors to systematically disregard human rights within the scope of security operations.[103]

Spyware infections are technically difficult to confirm, making the exact number of targeted individuals difficult to determine. In the media sector, for

[101] Morris and Veiberg, "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to Deliver Essential Public Services."
[102] UN Human Rights Council, *Surveillance and Human Rights: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,* A/HRC/41/35 (28 May 2019).
[103] Fionnuala Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach,* UN Human Rights Special Procedures, April 2023.

example, non-investigative journalists can be targeted simply because they communicate with sources already under surveillance. However, the most vulnerable targets are journalists who publish articles that threaten authoritarian regimes, such as reports exposing high-level corruption.[104] Azerbaijan, an oil-rich country on the Caspian Sea coast, is a prime example of where pressure on free speech and political dissent has been increasing since 2014. Khadija Ismayilova's investigation into the wealth of the country's ruling family made her a prime target for government surveillance. A forensic analysis released by Amnesty International's Security Lab and Forbidden Stories revealed that Ismayilova's phone had been periodically infected with Pegasus for nearly three years. This case demonstrates that journalists who expose corruption at the highest levels of power are the most vulnerable profile to multi-year spyware attacks.[105]

Shortly after the attack on Khadija Ismayilova's iPhone on 10 September 2019, the NSO Group announced a new corporate governance regime that it claimed was more transparent. These measures included: (1) updating operational policies to align with the UN Guiding Principles on Business and Human Rights; (2) establishing a Governance, Risk, and Compliance Committee; and (3) appointing an external expert panel to address human rights issues. The NSO Group argued that these initiatives would strengthen ethical business practices in the industry in which it claimed to operate.[106] However, the NSO Group failed to deliver on its commitment to placing human rights at the foundation of its corporate governance. In July 2021, the Pegasus Project, a consortium of sixteen global media outlets coordinated by Forbidden Stories, revealed that Pegasus was not only used by its clients to spy on suspected terrorists or criminals, as the NSO Group had promised. The investigation revealed that Pegasus had been used

[104] Fred Guterl, "Special Report: When Spyware Turns Phones Into Weapons," *Committee to Protect Journalists,* 13 October 2022, https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/ . Accessed on 18 January 2026.
[105] Phineas Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists," *Forbidden Stories,* 18 July 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/ . Accessed on 22 January 2026
[106] Laurent Richard and Sandrine Rigaud, *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* (New York: Henry Holt and Co., 2023).

extensively against more than 50,000 members of civil society, including human rights activists, journalists, academics, religious leaders, and lawyers.[107] The spread of commercial spyware such as Pegasus is not only a threat to human rights, but also a national security issue.[108]

According to an investigation by The Pegasus Project, published by the Forbidden Stories consortium in 2021, it was revealed that at least 180 journalists worldwide had been selected as potential targets by NSO Group clients. These findings confirm that while the company claims its products are used only to combat terrorism and serious crime, in practice, the surveillance technology is systematically used to stifle press freedom and monitor investigative journalism activities in various countries. These targets are spread across 20 countries, 10 of which are NSO Group clients. These government clients range from autocratic governments like Bahrain, Morocco, and Saudi Arabia to democratic governments like India and Mexico. In fact, the tools have spread across the globe, from Hungary and Azerbaijan in Europe to Togo and Rwanda in Africa. The Pegasus Project report shows that many of these governments have not hesitated to target journalists, human rights defenders, political opponents, businesspeople, and even heads of state with this invasive technology.[109]

The results of this investigation then elicited a response from the NSO Group, addressed to Forbidden Stories, stating that due to contractual and national security considerations, the NSO Group could neither confirm nor deny the identity of its government clients.[110] The map below shows the distribution of journalists targeted by the spyware.[111]

---

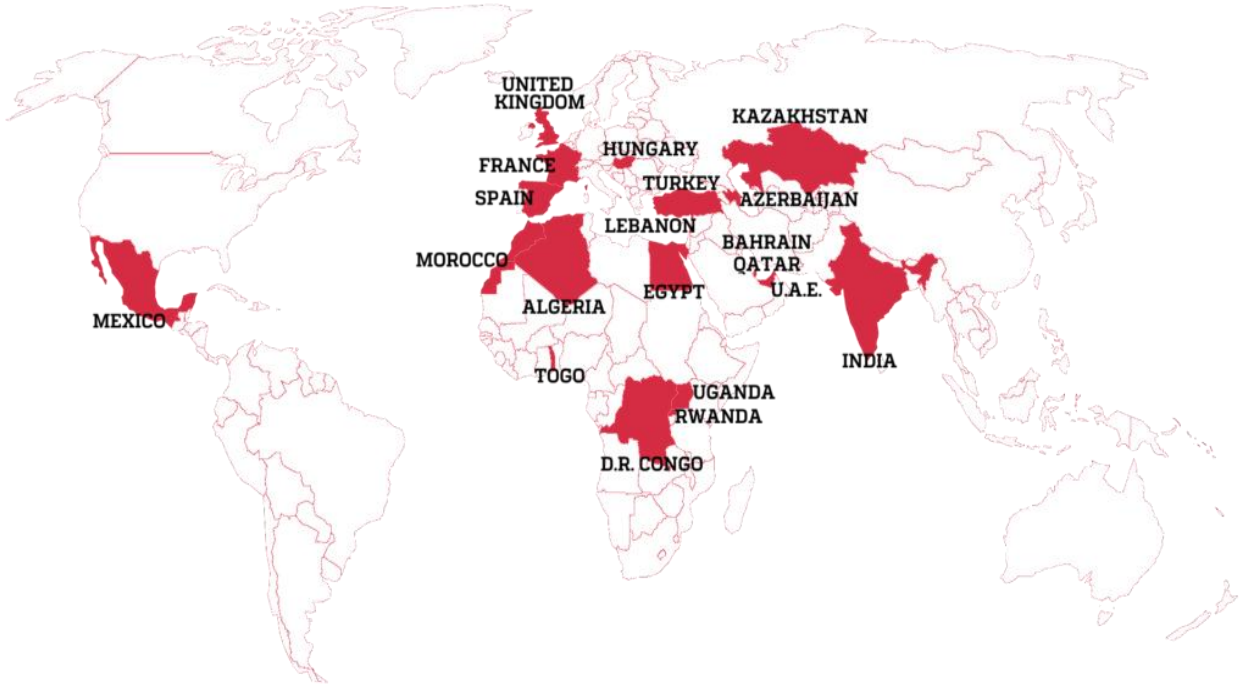
[107] Michael Silberman, "Policing Pegasus: The Promise of US Litigation for Commercial Spyware Accountability," *Georgetown Law Technology Review* 8, no. 1 (2024).

[108] In 2020 and 2021, devices belonging to officials at the UK's Foreign, Commonwealth and Development Office were hacked with Pegasus, along with a device located at the Prime Minister's residence, 10 Downing Street. A similar situation occurred in the United States. In March 2023, the White House said that at least fifty government employees were suspected or confirmed to have been targeted by commercial spy software. At the same time, President Joe Biden announced a ban on the use of commercial spy software across the government due to national security concerns. President Joe Biden mentioned Pegasus directly. See Silberman, "Policing Pegasus."

[109] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."

[110] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."

[111] Rueckert, "Pegasus: The New Global Weapon for Silencing Journalists."



In Morocco, for example, the Pegasus Project reported that journalist Soulaiman Raissouni was singled out for targeting before becoming editor-in-chief of Akhbar al-Youm, one of the country's few independent newspapers. The journalist is currently serving a five-year prison sentence for sexual harassment, which his supporters say was fabricated. The editor who replaced Raissouni, Taoufik Bouachrine, is also reportedly on the surveillance list. Taoufik Bouachrine is currently serving a 15-year prison sentence on multiple sexual misconduct charges, which local journalists and press freedom advocates believe was retaliation for his critical reporting.[112]

A Citizen Lab report found the use of spyware technology to target specific individuals in Mexico. The Mexican government obtained the spyware software and used it to spy on a human rights activist in the country and a journalist who

[112] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."

regularly reported on issues related to government corruption. The report noted that the surveillance occurred years after the first disclosure of the use of the Pegasus spyware in Mexico and after the Mexican president assured the public that the government was no longer using digital surveillance technology.[113] A similar case occurred in El Salvador, where spyware was used to threaten press freedom. The Knight First Amendment Institute at Columbia University filed a lawsuit against the NSO Group on behalf of journalists from El Faro.[114] The journalists believe that, based on the hacking pattern, they are being targeted by the increasingly repressive regime of Salvadoran President Nayib Bukele. Although El Salvador denies being a client of NSO Group, Citizen Lab and Amnesty International have verified the findings. NSO Group again claims that the findings of Citizen Lab and Amnesty International are unreliable.[115]

At a more extreme level, the use of spyware technology for mass targeting of civilians has been observed in Gaza, Palestine.[116] What is happening in Palestine reinforces the phenomenon of data colonialism. How digital technology transforms everyday life into a resource to be extracted for profit. Data colonialism creates a new social order in which human life is treated as something to be mined, tracked, and owned. The faces, voices, and movements of Palestinians are transformed into data to power predictive policing and autonomous targeting. Occupied Palestine is not only considered a disposable commodity, but also a computational raw material.[117]

Francesca Albanese's report refers to Project Nimbus and reveals that the

---

[113] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

[114] The Knight Institute explains that the El Faro journalist group brought its case to US court because the NSO Group offered its clients the ability to exploit vulnerabilities in US technology companies' software and services. The institute also notes that El Faro is widely read in the US and that one of the targeted journalists is an American citizen. See Jon Allsop, "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press," Columbia Journalism Review, 14 February 2023, https://www.cjr.org/the_media_today/pegasus_spyware_court_cases.php . Accessed January 20, 2026.

[115] Allsop, "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press."

[116] Suchitra Vijayan, "Technologies of Genocide: How Big Tech Profits From Mass Annihilation," *The Polis Project,* 20 August 2025, https://thepolisproject.com/listen/technologies-of-genocide-how-big-tech-profits-from-mass-annihilation/ . Accessed on 22 January 2026

[117] Vijayan, "Technologies of Genocide: How Big Tech Profits From Mass Annihilation."

primary funding source comes from the Israeli Ministry of Defense, with the involvement of Microsoft, Alphabet, and Amazon. These companies all provide Israel with near-full access to their cloud computing techniques and artificial intelligence technologies to enhance its capabilities in data processing, decision-making, surveillance, and analysis. In July 2024, an Israeli colonel described cloud technology as a weapon in the truest sense of the word. The role of technology companies is not limited to providing information to the Israeli occupation and its genocidal apparatus, but also extends to providing a "shield of immunity," as it protects crucial data that could serve as conclusive evidence before any international tribunal for war crimes. Albanese's report quotes Colonel Racheli Dembinsky, commander of the Israeli army's Computing and Information Systems Center, which is responsible for processing armed forces data, explaining that the army has become directly dependent on cloud computing storage and artificial intelligence services provided by global technology giants: Amazon Web Services, Google Cloud, and Microsoft Azure.[118]

Such use is not limited to authoritarian states or countries involved in armed conflict. Cases of spyware use have also spread to democratic countries in Europe, such as Greece, Hungary, France, Spain, Finland, Poland, Cyprus, and Belgium. Investigative reports indicate that several European countries have used Pegasus or similar spyware to spy on journalists, political opponents, and human rights defenders. Spyware is used for illegitimate purposes such as monitoring, blackmailing, intimidating, manipulating, and discrediting the opposition and critics, eliminating democratic oversight and a free press, and manipulating elections.[119]

A similar situation is also observed in the Indonesian context. Gatra Priyandita, a foreign policy and cyberpolitics expert at the Australian Strategic

[118] Vijay Prashad and Ubai Al-aboudi, "How the World Enriches from the Blood of the Palestinians," Progressive International, 17 November 2025, https://progressive.international/wire/2025-11-17-how-the-world-enriches-from-the-blood-of-the-palestinians/en/ . Accessed on 22 January 2026.

[119] Agnieszka Bień -Kacała, " Pegasus contra democratic process: experience from Europe," in *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World,* ed. Michał Balcerzak and Julia Kapelańska-Pręgowska (Cheltenham: Edward Elgar Publishing Limited, 2024).

Policy Institute (ASPI), stated that Indonesia uses spyware for legitimate national security purposes, such as counterterrorism. However, Priyandita issued a critical note:[120]

"There are numerous news stories and anecdotes about security forces misusing it to spy on journalists, prominent opposition figures, and civil society activists. The ability to acquire commercial spyware leads to a decline in civil liberties, and this situation is part of a broader trend. While spyware is only one potential method of repression, its use clearly facilitates and allows officials to abuse their power more freely."

The use and procurement of spyware inherently have legal implications for states. Under international human rights law, every state has a legal obligation to respect and protect human rights, including ensuring effective remedies or redress for violations. Furthermore, states are responsible for overseeing and ensuring that supplier companies adhere to human rights standards in conducting their business, in order to prevent the technology from being used for unlawful purposes. While states may delegate the provision of goods and services to the private sector, the obligation to comply with international human rights law commitments remains solely with the state and cannot be transferred. Therefore, the digital technology procurement process is a crucial modality for states to identify and mitigate the risks of human rights violations that may arise from the use of such technology in public services.[121]

[120] Tom Uren, "Amnesty Flags Possible Spyware Abuse in Indonesia," *Lawfare,* 17 May 2024, https://www.lawfaremedia.org/article/amnesty-flags-possible-spyware-abuse-in-indonesia . Accessed on 20 January 2026.

[121] Korzak, "Managing Commercial Spyware Through Export Controls: Lessons Learned from the Wassenaar Experience."

F. The Threat of Spyware to Democracy and Human Rights: The Construction of a Human Rights Norm Structure in Responding to the Dynamics of the Relationship between Technology and Human Rights

Steven Feldstein defines digital repression as the use of information and communication technologies to monitor, coerce, or manipulate individuals and groups. This is done to suppress activities or beliefs that challenge the state. Digital repression can be classified into several categories, namely: targeted surveillance (such as the use of spyware and data extraction technology), online censorship, social manipulation and disinformation, internet shutdowns, and targeted persecution of online users. Spyware remotely hacks targeted devices, while data extraction technology is used to access and extract information from devices in the physical possession of operators, which is now used by government officials at borders and ports of entry worldwide.[122]

According to the European Data Protection Supervisor, three key characteristics distinguish Pegasus from other spyware, potentially causing unprecedented risks and damage. These risks not only threaten fundamental individual freedoms but also democracy and the rule of law. This is due to the spyware's capabilities:[123]

1) Gaining full access to the targeted device;

2) Conducting zero click attacks;

3) Leaving little or no trace.

The unauthorized use of Pegasus can disrupt every element of the democratic process. By targeting journalists and activists, this spyware hinders citizens' efforts to hold governments and other public institutions accountable. Furthermore, surveillance has opened the door to repression, manipulation, blackmail, falsification, and defamation. These hostile actions can have further

[122] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."
[123] Sartor and Loreggia, "The Impact of Pegasus on Fundamental Rights and Democratic Processes."

consequences for civil society and political participation. Citizens may withdraw from political engagement and the expression of their views and opinions. The use of spyware can also undermine the integrity of elections, or at least make them unfair. This occurs because those in power gain illegal access to confidential information about their political opponents. The collected data is then manipulated and used to attack opposition candidates through smear campaigns. Such campaigns can have further consequences, potentially leading to candidates being disqualified from running for office.[124]

According to Winnona DeSombre et al., spyware is one of the most dangerous types of offensive cyber capabilities. This is because spyware can utilize computing devices and techniques to deeply exploit vulnerabilities in computer networks and systems. These capabilities are developed and operated by various actors, ranging from government institutions and criminal networks to Intrusion-as-a-Service (IAS) providers, who sell computer network hacking services to third parties.[125] Over the years, several IAS groups have impersonated the private sector and engaged with nation-states to sell their sophisticated products and services. These groups have proliferated their offensive cyber capabilities due to the semi-regulated nature of the market.[126]

The global spyware industry continues to expand as companies like Candiru, Cytrox, and RCS Labs continue to operate. In June 2022, Google researchers warned victims in Kazakhstan and Italy of a sophisticated RCS Labs program called Hermit. This device is capable of not only stealing data but also recording voices and making calls autonomously. The emergence of Hermit spyware demonstrates how threat actors, often operating as state-sponsored

[124] Bie ń -Kaca ł a, " Pegasus contra democratic process: experience from Europe. "

[125] Access-as-a-service (AaaS) is a growing extension of the cybercrime-as-a-service model, where malicious actors offer access points to business networks as a product. The perpetrators, known as Initial Access Brokers (IABs), operate opportunistically, exploiting identified vulnerabilities to generate profit. See, UN Interregional Crime and Justice Research Institute (UNICRI) and UN Office of Counter-Terrorism (UNOCT), *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks,* 2024.

[126] Maira Cardillo, Sina Fischer, and Aditi Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People* (Geneva: Geneva Graduate Institute and CyberPeace Institute, 2023).

entities, are shifting to new surveillance technologies and tactics following the revelations of the NSO Group's Pegasus scandal. Previously, NSO Group products were known to have been misused by repressive regimes to attack activists and civil society organizations, and were even implicated in the murder of journalists.[127]

The industry's lack of regulation makes spyware abuse even more difficult to prevent. NSO Group's general counsel, Chaim Gelfand, declined to name specific clients when speaking before the European Parliament's spyware investigation committee in June 2022. NSO Group argued that its sale of Pegasus to governments was a legitimate activity:[128]

"This system is sold to save lives, but this device can be misused"

Meanwhile, the NSO Group itself does not target individuals through its Pegasus spyware, but rather provides a means for states to conduct surveillance. The NSO Group acknowledges this potential danger. NSO Group's admission, contained in one of its company reports, states that it is fully aware that if customers misuse one of its products, it could harm the human rights of individuals not involved in serious crimes or terrorism, particularly the right to privacy or freedom of opinion and expression.[129] The NSO Group states that the purpose of developing Pegasus is to help authorities apprehend criminals who may communicate through encrypted messaging services. However, Pegasus devices can also be used for illegitimate purposes. Civil society organizations and investigative journalists have documented dozens of cases of Pegasus spyware that indicate human rights violations.[130]

---

[127] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."
[128] Guterl, "Special Report: When Spyware Turns Phones Into Weapons."
[129] Silberman, "The Spyware Exception: How the Foreign Sovereign Immunities Act Protects Foreign State Malware Attacks."
[130] Caitlin Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware," Georgetown Journal of International Affairs, 4 September 2024, https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/ . Accessed on 25 January 2026.

More than 500 companies currently develop, market, and sell surveillance tools to governments. Therefore, efforts are needed to regulate an industry that has expanded beyond the NSO Group. The UN Special Rapporteur on freedom of opinion and expression, David Kaye, warned that the current regulatory regime for commercial spyware is wholly inadequate:

"The commercial private surveillance industry is a free-for-all that creates an ecosystem where states and industry collaborate in the deployment of technologies that cause direct and regular harm to individuals and organizations vital to democratic life, namely journalists, activists, opposition figures, lawyers, and others."

Under the International Covenant on Civil and Political Rights, governments may not unlawfully or arbitrarily interfere with an individual's freedoms of privacy, expression, assembly, and association.[131]

The use of Pegasus has raised concerns not only about the safety of journalists and media professionals and its chilling effect on investigative journalism, but also about the erosion of democratic norms and the rule of law. Specifically, the UN in 2021 drew special attention through the UN High Commissioner for Human Rights, Michelle Bachelet, who stated:[132]

"Concerns about the extremely dangerous implications of the use of Pegasus spyware for human rights. The technology's surveillance capabilities pose serious risks to freedom of opinion and expression, which are fundamental to democracy."

The UN Special Rapporteur on the Right to Freedom of Opinion and Expression points to the human rights legal framework that protects against targeted surveillance. The International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights protect everyone's right to privacy,

[131] Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware."
[132] "Slovakia: Use of Pegasus a Threat to Democracy and Human Rights," *Article19,* September 9, 2024, https://www.article19.org/resources/slovakia-use-of-pegasus-a-threat-to-democracy-and-human-rights/#:~:text=The%20European%20Union%20Agency%20for , use%20of%20Pegasus%20in%20Slovakia . Accessed on 6 January 2026.

opinion and expression. Article 19 of both instruments protects everyone's right to hold opinions without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Article 17(1) of the Covenant, echoing Article 12 of the Universal Declaration of Human Rights, states that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence. Privacy and expression are intertwined in the digital age, with online privacy serving as a gateway to the safe exercise of freedom of opinion and expression. Article 17 permits interference with the right to privacy only if it is permitted by readily accessible and appropriate domestic law and complies with the requirements of the International Covenant on Civil and Political Rights, pursues a legitimate purpose and meets the tests of necessity and proportionality. Article 19 sets out a three-part test requiring that restrictions must be provided by law and necessary to protect the rights or reputations of others, national security or public order, or public health or morals.[133]

The Special Rapporteur further referred to the Human Rights Committee in his 2017 concluding observations on Italy's sixth periodic report. The Committee stated that the right to privacy requires a robust and independent oversight system regarding surveillance, wiretapping, and hacking, including ensuring that the judiciary is involved in authorizing such actions and provides effective remedies to those affected by abuse. Where possible, following a surveillance incident, States should notify anyone who has been the target of the surveillance or whose data has been compromised. The General Assembly, in resolution 73/179, emphasized that surveillance of digital communications must be consistent with international human rights obligations and must be conducted under a legal framework that must be publicly accessible, clear, precise, comprehensive, and non-discriminatory.[134]

UN Special Rapporteur on Freedom of Peaceful Assembly and of Association pushes all countries to promote the use of and access to a free, open,

[133] UN General Assembly, *The right to privacy in the digital age,* UN Doc. A/RES/73/179 (17 December 2018).
[134] UN General Assembly, *The right to privacy in the digital age,* UN Doc. A/RES/73/179.

interoperable, reliable, and secure internet, by facilitating international cooperation aimed at developing media, information, and communication facilities in all countries, while respecting and protecting human rights, including the freedoms of peaceful assembly and association, and the right to privacy, and refraining from imposing undue restrictions. These restrictions include internet shutdowns, arbitrary or unlawful surveillance, or online censorship.[135] The Special Rapporteur expresses deep concern at the numerous cases in which peaceful assembly, including peaceful protests, has been met with repressive measures. Such repression includes the unlawful use of force by law enforcement officials, the misuse of non-lethal weapons, and arbitrary arrest and detention. The Special Rapporteur also highlights the practice of torture, cruel, inhumane treatment, enforced disappearances, and illegal surveillance. Furthermore, digital repression, such as internet shutdowns and network restrictions, frequently targets protesters, human rights defenders, journalists, and minority and other vulnerable groups exercising their rights to freedom of peaceful assembly and association.[136]

The Special Rapporteur in previous reports expressed concern about arbitrary and unlawful surveillance, both in physical and online spaces, of individuals engaged in peaceful protests, including through the use of CCTV and aerial surveillance vehicles, as well as through the use of new and emerging digital tracking tools, such as biometric technologies, including facial and emotion recognition and international mobile subscriber identity capture (*stingray*). Furthermore, the Special Rapporteur called on States to refrain from the export, sale, transfer, use or maintenance of surveillance goods and technologies that may be used to violate or abuse human rights, including in the

[135] UN Human Rights Council, *The Right to Freedom of Peaceful Assembly and of Association,* Resolution A/HRC/50/L.20 (4 July 2022).
[136] UN Human Rights Council, *The Right to Freedom of Peaceful Assembly and of Association,* Resolution A/HRC/50/L.20.

context of meetings. The Special Rapporteur even urged a global moratorium on the sale, transfer and use of such targeted surveillance technologies.[137]

Fionnuala Ní Aoláin in her capacity as Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism narrated the potential misuse of surveillance tools that go beyond their purpose of countering terrorism:[138]

"Advanced surveillance technologies developed for counter-terrorism and national security purposes are increasingly becoming the focus of international attention due to empirical evidence from a series of revelations showing the use of these devices to spy on politicians, journalists, human rights activists, lawyers, and ordinary citizens who have no ties to terrorism and do not pose a national security threat.

Intrusive covert technologies for surveillance of the content of individuals' digital communications and other information, including metadata (location, duration, source, and contacts) commonly known as spyware have proliferated internationally out of control and pose a significant risk to the promotion and protection of human rights."

The Special Rapporteur then refers to the case of the misuse of the Pegasus spyware device:[139]

"These profound challenges are illustrated by the scandal surrounding the use of Pegasus by repressive regimes, a surveillance software program produced by the cyberintelligence firm NSO Group."

---

[137] UN Human Rights Council, *The Right to Freedom of Peaceful Assembly and of Association,* Resolution A/HRC/50/L.16 (30 June 2022).

[138] Fionnuala Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,* Special Rapporteur Report on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UN Doc. A/HRC/52/39 (1 March 2023).

[139] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,* UN Doc. A/HRC/52/39.

Furthermore, the Special Rapporteur emphasizes that a human rights analysis of the use of spyware in the context of counter-terrorism must at least ensure that such devices:[140]

1) Allow users to specifically target certain data and metadata, rather than automatically monitoring and recording all data and metadata;

2) Avoid automated access to data relating to the contacts of targeted individuals, unless the user specifically requires such additional information for investigative purposes;

3) Create an irremovable, permanent, and uneditable audit record of what actions the spyware user has taken, including any data/metadata tampering/modification, when it occurred, and by whom, so that the use of the software can be verified, and its compliance with human rights can be assessed after the fact by judicial authorities. Spyware that fails to exhibit such features, even if strictly regulated, cannot meet human rights requirements.

The Situation Report on the Right to Privacy by the Office of the United Nations High Commissioner for Human Rights (UNHRC) articulates the threats to human rights that arise from decisions based on automated decision-making systems, predictive analytics, and biometric recognition systems that contain bias or are applied in contexts that favor or disproportionately affect certain groups. Surveillance technologies have historically been used to target specific groups. Biometric recognition systems are used to identify and track peaceful protesters and dissidents and discriminate based on political opinion. The arbitrary application of surveillance technologies can also impede the exercise of freedoms and other rights. A range of surveillance activities carried out by states and businesses pose a significant threat to the right to privacy and other human rights.[141] Surveillance is used in armed conflicts with severe impacts on

[140] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,* UN Doc. A/HRC/52/39.
[141] Office of the United Nations High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age,* UN Doc. A/HRC/60/45 (29 August 2025).

civilians and civilian objects. Widespread surveillance risks being misused for racial targeting (racial profiling) and identifying and tracking individuals for discriminatory purposes, for example, based on their political beliefs. Even when serving legitimate purposes, from managing complex urban environments to facilitating access to public services, surveillance often fails to meet the requirement of proportionality. This poses serious challenges to the rights to privacy and freedoms that are at the heart of open, democratic societies.[142] The UN human rights system has consistently raised concerns about surveillance by government agencies, including mass and targeted interception of communications, access to and collection of communications data, and intrusion into electronic devices through hacking. This also includes increased surveillance in public spaces, both online and offline, which is being strengthened through the use of biometric technologies and artificial intelligence-based systems.[143]

Intrusion through surveillance devices affects an individual's right to privacy. The Office of the United Nations High Commissioner for Human Rights (OHCHR) defines surveillance as arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence. Surveillance can violate an individual's right to freedom of association and expression. Under international human rights law, three principles are crucial for assessing the legality of surveillance measures.[144]

First, does domestic law permit surveillance? In this regard, Frank La Rue's successor, David Kaye, issued a report in 2019 emphasizing that legal norms must be formulated precisely enough to allow individuals to regulate their behavior in accordance with them and must be publicly accessible. Legal norms must not be vague or overbroad, allowing government officials unfettered discretion. The

[142] OHCHR, *The Right to Privacy in the Digital Age,* UN Doc. A/HRC/60/45.
[143] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Mapping report: human rights and new and emerging digital technologies,* UN Doc. A/HRC/56/45 (20 August 2024).
[144] Steve Feldstein, "The Global Expansion of AI Surveillance," *Carnegie Endowment for International Peace,* September 17, 2019, https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance .

legal framework itself must be publicly accessible, clear, precise, comprehensive, and non-discriminatory.

Second, whether the surveillance measures meet international legal standards according to the principles of necessity and proportionality, which will limit surveillance to situations that are strictly and demonstrably necessary to achieve a legitimate aim.

Third, whether the interests justifying the surveillance measures are legitimate. There is considerable disagreement over what constitutes legitimate surveillance and what constitutes an abuse of power. While governments generally justify surveillance on grounds of national security or public order, the Office of the United Nations High Commissioner for Human Rights (OHCHR) warns that such restrictions can unfairly or arbitrarily limit citizens' rights to freedom of opinion and expression. David Kaye argues that legitimate surveillance requires states to demonstrate the risk that a particular expression poses to a specific interest in national security or public order. Furthermore, a robust and independent oversight system is needed that entrusts the judiciary with validating relevant surveillance measures and providing remedies in cases of surveillance abuse. Kaye further adds that legitimate surveillance should only be applied when the interests of the entire nation are at stake and should exclude surveillance conducted solely for the benefit of the government, regime, or ruling group.

Various regional mechanisms emphasize the need for strict regulation, the establishment of oversight mechanisms, and the implementation of accountability measures to prevent the misuse of Pegasus and similar spyware by governments. This is based on the urgent need to protect human rights, democracy, and the rule of law from the threats of increasingly sophisticated surveillance technologies:[145]

[145] Cardillo, Fischer, and Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

1) Report of the Council of Europe's Parliamentary Assembly A 2023 report highlighted the sale of Pegasus to at least 14 European Union countries, including Belgium, Germany, Hungary, Luxembourg, the Netherlands, Poland, and Spain. The report called for a moratorium on the sale and use of the spyware until an adequate legal framework and safeguards are in place.

2) The European Parliament's Committee of Inquiry (PEGA Committee), tasked with investigating the use of Pegasus and similar spyware, found evidence of misuse in Poland, Hungary and Greece. The Committee's draft recommendations condemned the unauthorized use of spyware by member state governments and called for common EU standards to regulate the use of such surveillance tools.

3) The European Union Agency for Fundamental Rights emphasized that the use of Pegasus poses a threat to fundamental rights guaranteed in the EU Charter, such as freedom of expression, freedom of the press, and freedom of association. The agency also raised issues regarding the effectiveness of EU export controls and human rights protections in the procurement of spyware from third countries.

The PEGA Committee urges governments to limit the procurement and use of spyware for national security purposes through accountability measures, such as independent judicial oversight or audits to prevent secondary misuse. The PEGA Committee further urges increased transparency by annually publishing high-level statistics that include (1) the number of spyware targets, including their general purpose, nationality, and other demographic variables; (2) the percentage of spyware targets that result in criminal prosecution; (3) the identity of any third parties who receive access to spyware technology; and (4) a description of procedures for protecting human rights throughout the surveillance cycle. Governments should also notify targets after surveillance ends and provide avenues for individuals to seek justice in the event of human rights

violations.[146]

Spyware has the ability to perform comprehensive intrusion on infected devices. As a result, all data on the phone can be extracted or monitored. These tools can be used to collect further data from the external environment and interfere with the device's content and sent messages. In this context, Pegasus is difficult to detect and track. However, devices infiltrated by spyware exhibit several symptoms, such as increased data usage, sudden battery drain, and poor or slow device performance. These symptoms are why Pegasus and other spyware tools, such as Cytrox's Predator or Candiru, are so tempting to use against individuals other than terrorists and criminals, potentially endangering their human rights, particularly the rights to privacy and data protection, as well as freedom of speech, association, and assembly. Surveillance, whether mass or targeted, can have a chilling effect on various societal activities, including those in private areas such as health and religion. This ultimately triggers widespread self-censorship. Surveillance has undermined the sense of security and fueled massive public distrust, which fundamentally poses a real threat to the sustainability of democracy.[147]

Spyware is typically used in conjunction with other tools of digital oppression. There are also other socioeconomic and structural factors at play in each person's situation that cannot be mitigated by the targeted (profiled) user. Most individuals targeted by spyware experience a chilling effect, such as self-censorship and increased word choice to avoid government repression, ranging from defamation and job loss to criminalization. Targeted individuals then become hesitant to socialize and connect with others, finding it more difficult to live authentically because they feel they are under the shadow of surveillance. In some of the most extreme examples, spyware has led to arbitrary deprivation of life or prolonged imprisonment in appalling conditions.[148]

The murder of Jamal Khashoggi is clear evidence of how spyware poses a

[146] Chin-Rothmann, "Cyber Mercenaries: Limiting Government Use of Commercial Spyware."
[147] Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law."
[148] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."

deadly threat to democracy and human rights. The Pegasus Project identified that Jamal Khashoggi's murder was inextricably linked to the intrusion of private communications linked to the use of spyware technology. In this case, Jamal Khashoggi's other rights were violated, including the right to life, the right to be free from torture and physical violence, the right to freedom of expression, and the right to privacy.[149] In this case, NSO clients used Pegasus software that can turn phones into surveillance devices with embedded microphones and cameras that are activated without the user's knowledge.[150]

It's undeniable that we now live in a world of mass surveillance due to the widespread use of facial recognition technology and online tracking by both governments and tech companies. However, targeted surveillance has a slightly different nature. It involves the use of technology to spy on specific individuals. Often, these targets are journalists, bloggers, and activists who speak out for the truth, expose corrupt deals, demand electoral reform, or promote the right to privacy. In many cases, governments use sophisticated cyber tools to conduct illegal surveillance, such as through seemingly harmless missed calls, personalized text messages, or involuntary redirects to malicious websites.[151] In 2020, Amnesty International released a report on the use of spyware to target human rights defenders. The report revealed that figures such as Ahmed Mansoor (United Arab Emirates), Maati Monjib (Morocco), and Yahya Assiri (Saudi Arabia) had been targeted in surveillance operations.[152]

Pegasus also targeted Mexican journalist Javier Valdez Cárdenas. Valdez Cárdenas was a senior journalist and founder of the Río Doce newspaper. He was known for investigating drug cartels and violence in Mexico. In May 2017, the journalist was shot dead near his office. Two of his colleagues, Andrés Villarreal and Ismael Bojórquez, received text messages containing malicious links

[149] Megiddo, "Spyware Exports: Recognizing the Limits of Human Rights Law."
[150] Stephanie Kirchgaessner, "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests," *The Guardian,* 18 July 2021, https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus . Accessed on 6 January 2026.
[151] Amnesty International, "When Is Targeted Surveillance Wrong?"
[152] Amnesty International, "When Is Targeted Surveillance Wrong?"

designed to infect their phones. A Citizen Lab report noted that at least 24 people in Mexico were targeted by similar attacks, although not linked to criminal activity or terrorism.[153] Following a joint investigation into the use of Pegasus spyware against Galina Timchenko, co-founder, CEO, and publisher of Meduza, Access Now, Citizen Lab and independent digital security expert Nikolai Kvantiliani have revealed how at least seven other Russian, Belarusian, Latvian, and Israeli journalists and activists have been targeted by NSO Group's Pegasus spyware in the European Union.[154]

The use of spyware, particularly Pegasus, to target pro-democracy movements has been evident in Thailand and Jordan. In Thailand, from October 2020 to November 2021, approximately 30 activists, academics, lawyers, and NGO workers were targeted during widespread pro-democracy protests. In Jordan, human rights defenders have had to work in an intimidating environment. It was later revealed that several of them, including lawyers and journalists, had been spied on using Pegasus spyware between August 2019 and December 2021. Other patterns of Pegasus or spyware use can be linked to authoritarian government tendencies and human rights violations. This was observed in Togo and El Salvador. In El Salvador, in 2021, surveillance of journalists and civil society activists was discovered. This case serves as a basis for mapping the pattern of governments that frequently misuse this technology. This pattern is shaped by a variety of interconnected factors, from the presence of an autocratic president obsessed with digital technology, a track record of media intimidation, to a climate of insecurity and chronic human rights violations. This ecosystem also encompasses the activities of intelligence agencies, the police, and the private security sector, operating without legal oversight, all of which are intertwined with

[153] Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague," *The Citizen Lab,* 27 November 2018, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/#:~:text=Key%20Findings,to%20prevent%20the%20continuing%20abuse.Accessed on November 2025

[154] "Exiled, Then Spied on: Civil Society in Latvia, Lithuania, and Poland Targeted With Pegasus Spyware - Access Now," *Access Now,* 30 May 2024, https://www.accessnow.org/publication/civil-society-in-exile-pegasus/ . Accessed on 16 January 2026.

a long history of corruption, state violence, and authoritarianism.[155]

As it developed, the pattern of spyware use is not only directly targeted towards individual devices, but also hijacked the infrastructure of global technology companies to reach their targets. Even WhatsApp and its parent company Facebook sued the NSO Group for using WhatsApp servers to send the Pegasus spy software to the devices of 1,400 users. In a lawsuit filed in the Northern District Court of California in October 2019, Meta accused the NSO Group of violating the US Computer Fraud and Abuse Act (CFAA), the California Comprehensive Data Access and Fraud Act, as well as contract law and property infringement. The Citizen Lab revealed that more than 100 of these attacks targeted members of civil society, including human rights activists, journalists, dissidents, lawyers, and even religious leaders.[156] Court documents specifically listed the countries where the victims infected by Pegasus were located. The highest number of victims were in Mexico (456 people), India (100), Bahrain (82), Morocco (69), Pakistan (58), Indonesia (54), and Israel (51). Additionally, according to a table titled " Number of victims by country" submitted to the court by WhatsApp, victims were also identified in countries such as Spain (21 victims), the Netherlands (11), Hungary (8), France (7), the United Kingdom (2), and the United States (1). One victim was in the Czech Republic.[157]

Moreover, referring to the Report entitled "From Economy of Occupation to Economy of Genocide " on 2 July 2025, compiled by the UN Special Rapporteur on the situation of human rights in the Palestinian Territories, genocide in the Gaza region is made possible by and benefits corporate actors, especially technology giants, including surveillance companies. Corporate interests are suspected of supporting the dual logic of Israeli settler colonialism through displacement and

[155] Bie ń -Kaca ł a, " Pegasus contra democratic process: experience from Europe. "
[156] Access Now, "Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in US courts," 23 December 2020, https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/ . Accessed on 16 January 2026.
[157] Barbora Šturmová, "Pegasus Spyware Targeted Over 1,400 WhatsApp Users, Including in Hungary and Czechia, Court Documents Show," *VSquare,* 20 November 2024, https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/ . Accessed on 16 January 2026.

replacement.[158] Surveillance and detention technologies, traditionally used to enforce segregation/apartheid, have evolved into tools to target the Palestinian population. Repression against Palestinians is increasingly automated, with technology companies providing dual-purpose infrastructure to integrate mass data collection and surveillance. Israel's claims of security needs have fueled unprecedented developments in prison and surveillance services, ranging from closed-circuit television (CCTV) networks, biometric surveillance, high-tech checkpoint networks, "smart walls" and drone surveillance to cloud computing, artificial intelligence and data analytics to support military personnel in the field.[159]

More broadly, targeted digital surveillance has a unique and disproportionate impact on women, particularly women human rights defenders, who can also be targeted by the state through physical repression. Given that paid spyware allows complete control over infected devices, including access to cameras, microphones, stored photos/videos, messages, and call logs, there are significant risks for targeted women. This personal information can be used to facilitate various acts of technology-enabled gender-based violence, such as blackmail or doxxing, which have a serious and disproportionate impact on targeted women. Furthermore, the targeting of female members of civil society causes some targets to live in a constant state of fear and become increasingly isolated and restricted in their work and social lives.[160] Furthermore, the impact of spyware can extend beyond the targeted individual and can affect other members of society. For example, targeted surveillance can undermine the ability of civil society to carry out activities in the public interest, including conducting investigations, engaging in human rights and political activism, and interacting with their professional and personal networks.[161]

---

[158] Francesca Albanese, *From economy of occupation to economy of genocide,* Special Rapporteur report on the situation of human rights in the Palestinian territories occupied since 1967, UN Doc. A/HRC/59/23 (2 July 2025).
[159] Albanese, *From economy of occupation to economy of genocide,* UN Doc. A/HRC/59/23.
[160] Siena Anstis & Jillian Sprenger , Civil society and access to justice: challenges of seeking remedies in the global fight against spyware, The International Journal Of Human Rights, 2025
[161] Ibid.

G. David vs. Goliath: The Powerless Public vs. the Gigantic Power of Technology Corporations in the Framework of the Business Norms and Human Rights Landscape

The global spyware market is estimated to be worth $12 billion, with governments and law enforcement agencies as primary customers. These tools have the ability to exploit zero-day vulnerabilities, security holes unknown to system developers. Google notes that more than half of zero-day exploits targeting its products are closely related to the commercial spyware industry.[162] The global spyware market is currently dominated by private companies, such as the NSO Group, which commercializes surveillance technology to governments with minimal oversight. While NSO claims its products are aimed at combating terrorism and crime, numerous reports have shown widespread abuse against civilians. The murders of Jamal Khashoggi and Javier Valdez Cárdenas highlight the lack of oversight mechanisms for these companies. The limited global regulatory environment exacerbates this problem, allowing the export of spyware to authoritarian regimes without clear accountability.[163]

The spyware market is growing rapidly alongside increasing digitalization. However, this growth is not accompanied by an adequate policy framework to regulate transactions between states, intelligence agencies, and the private cybersecurity sector. This situation is fueled by the tendency of state institutions and companies to keep the market unregulated in order to maintain profits from a lack of transparency and oversight.[164] This allows intelligence agencies and the military to purchase spyware packages to infect and spy on critics, human rights activists, lawyers, and journalists. Consequently, the spyware market has

---

[162] Mailyn Fidler, "Sanctions for Spyware," Lawfare, 13 June 2024, https://www.lawfaremedia.org/article/sanctions-for-spyware . Accessed on 25 January 2026.

[163] Kyle Volpi Hiebert, "The Growing Global Spyware Industry Must Be Reined In," *CIGI,* 27 March 2023, https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/ . Accessed on October 2025.

[164] Cardillo, Fischer, and Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

continued to grow significantly over the past ten years.[165]

Manufacturers of spyware and other cyber surveillance devices can be broadly divided into two groups: (1) manufacturers producing devices related to local intelligence processes and data storage; and (2) manufacturers producing devices related to device hacking methods. Companies in this industry vary in their operational scale, as well as their level of awareness of export control mechanisms, international sanctions, and the accompanying legal obligations. Geographically, the production of spyware and other cyber surveillance technologies is concentrated in Europe. Based on mapping by SIPRI (Stockholm International Peace Research Institute), there are 188 companies spread across 31 countries operating in this industry. Of the total manufacturers, 51% are located in 19 European countries, 22% in three countries in the Americas, 13% in three countries in the Middle East, and 13% in five countries in Asia and Oceania. The spread and misuse of spyware and other cyber surveillance devices pose a serious threat to human rights and national security. Numerous reports have documented how a number of countries have used spyware to commit serious violations of international human rights law. Furthermore, civil society organizations have highlighted the use of this technology in the context of armed conflict, potentially violating international humanitarian law.[166]

Based on their implementation patterns, spyware operations can be divided into two main categories. *First*, internal national operations and the activities of Advanced Persistent Threat (APT) groups; these are operations run by state actors with the capacity to conduct independent and sustained intrusion attacks. *Second*, operations facilitated by commercial spyware vendors, where states purchase technical capabilities from private parties. Operations in the first category are often conducted by highly capable states, such as the National Security Agency's special access operations group, Israel's Unit 8200, and similar actors from China or Russia that receive direct or indirect government support.

---

[165] Cardillo, Fischer, and Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

[166] Mark Bromley and Giovanna Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint,* SIPRI Report (Stockholm: SIPRI, September 2025), http://doi.org/10.55163/GVXO6716 .

Operations in the second category are conducted using off-the-shelf hacking technology purchased from private security firms. These products do not require state actors to have the internal capacity to develop or conduct cyberattacks or surveillance. Instead, governments purchase these capabilities directly from the companies, which provide after-sales support, such as technical upgrades, product updates, training, and customer service. The emergence of the commercial spyware sector has given countries access to sophisticated surveillance tools that would be difficult to obtain through independent channels.[167]

The emergence of commercial spyware poses unique threats due to its operational characteristics and intended use. This technology is marketed as a legitimate solution for law enforcement to combat crime by granting access to sensitive data, such as instant messages, calls, photos, emails, and browsing history. Mobile phones are the primary target because these devices are personal and serve as the center of users' daily communications. However, there are also variants that target desktop devices, such as Candiru, also known as Karkadann, which has been detected active since at least 2020.

While democratic countries generally regulate the use of spyware through legal frameworks designed to protect citizens' rights and prevent mass surveillance, these protections are often limited to domestic jurisdictions and are vulnerable to degradation by regime shifts toward authoritarianism. Meanwhile, in many other countries, the absence of legal protection mechanisms leaves the population highly vulnerable to unregulated surveillance practices. While several democratic countries regulate the use of spyware through legal frameworks designed to protect citizens' rights and prevent mass surveillance, these protections are often limited to domestic jurisdictions and are vulnerable to degradation by regime shifts toward authoritarianism. Meanwhile, in many other countries, the absence of legal protection mechanisms leaves the population

[167] Feldstein and Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses.*

highly vulnerable to unregulated surveillance practices.[168]

However, according to Gail Horak, specific research on commercial spyware is still lacking. is limited for several reasons. *First*, commercial spyware is usually sold and purchased through nondisclosure agreements. *Second*, spyware is used covertly by government operators who want to remain undetected on target computers for as long as possible. *Third*, this technology is also relatively new. Commercial spyware has only been developed in the last decade and has only come to light through leaks, hacks, investigative reporting, and digital forensic analysis in recent years. The existence of internal government-created spyware, also known as advanced persistent threats, has also only been revealed indirectly.[169]

In the context of commercialization, Elaine Korzak broadly defines commercial spyware technology as a combination of hardware, software, and technical expertise used to covertly monitor, exploit, or analyze data. This definition encompasses the entire spectrum of data activity, whether stored, processed, or transferred through information and communications technology infrastructure. In this context, information and communications technology can include devices such as computers and mobile phones, or entire telecommunications networks.[170]

The commercialization of espionage and surveillance tools, once the exclusive domain of states but now shifting into commercial commodities, has become a major concern for the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms in counterterrorism. In her report, the Special Rapporteur stated:[171]

---

[168] Maxime Arquillière et al., *Predators for Hire: A Global Overview of Commercial Surveillance Vendors,* Sekoia, 2025, https://blog.sekoia.io/predators-for-hire-a-global-overview-of-commercial-surveillance-vendors/ .
[169] Horak, "Personal Details Exposed: Spyware and Human Rights in the Middle East and North Africa."
[170] Korzak, "Managing Commercial Spyware Through Export Controls: Lessons Learned from the Wassenaar Experience."
[171] Fionnuala Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism,* UN Doc. A/HRC/52/39 (1 March 2023).

"While in the past, espionage and surveillance technologies tended to be the exclusive preserve of government agencies and in-house technical experts, in the modern era, most of the surveillance equipment used by state agencies is acquired from the private sector. Private cybersecurity companies responsible for tools with such capabilities include Israel-based NSO, Quadream, and Candiru/Saito Tech; UK-based Gamma International; Germany-based Vilicius Holding and Trovicor; France-based Qosmos and Amesys; Italy-based Area SpA and Hacking Team/Memento Labs; Cytrox, which has divisions in Hungary, Israel, and North Macedonia; US companies CyberPoint, Narus (a Boeing subsidiary), Blue Coat Systems, and Cisco Systems; and the UAE company DarkMatter."

Therefore, the Special Rapporteur urges that the activities of these businesses and multinational corporations be regulated, in line with States' obligations regarding the regulation of the business sector, to prevent human rights violations.[172] The UN High Commissioner for Human Rights similarly stated that a better, human rights-based system is needed to regulate the trade in spyware, including mechanisms to hold private spyware manufacturers accountable for human rights violations by legally requiring the companies involved to meet: (1) human rights responsibilities; (2) be significantly more transparent regarding the design and use of products; and (3) implement more effective accountability measures. The High Commissioner also called for a suspension of trade in surveillance technology to allow States to strengthen export and control regimes, and to improve legal frameworks guaranteeing privacy.[173] Similar calls were made by the UN Special Rapporteur on the promotion and protection of the right to freedom of expression, the UN Special Rapporteur on the situation of human rights defenders, the UN Special Rapporteur on the right to freedom of peaceful assembly and association, and members of the UN Working Group on Business and Human Rights. The mandate holders of the Special Procedures stated: (1) that they raised concerns about the harms posed

[172] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism.*
[173] Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach.*

by surveillance technology to human rights; (2) urge the international community to develop a strong regulatory framework to prevent, mitigate and remediate the negative impacts of surveillance technology on human rights; and (3) impose a moratorium on the sale and transfer of such technology.[174]

The UN's concerns and calls for a moratorium are a direct response to the increasingly out of control transformation of the surveillance industry. A commercial surveillance vendor ecosystem emerged and strengthened its significant industrialization process between 2016 and 2021. Commercial surveillance vendors are private companies or groups of companies that develop, maintain, and sell spyware to clients, typically government agencies. These vendors' activities include vulnerability research or acquisition, exploit development, digital forensics, command and control infrastructure, or client training, all of which are typically included or offered as add-ons in a complete package. This evolution is evident in vendor offerings, which are shifting from isolated technical components to fully integrated solutions. Initially, vendors focused on providing single tools, such as spyware implants or traffic interception modules. Along with this evolution, new actors, such as NSO, have been selling turnkey solutions to government agencies. These solutions encompass the complete infection chain, including intrusion vectors, command and control infrastructure, and data exfiltration, with user-friendly interfaces featuring dashboards, multilingual support, and geolocation capabilities. The development of this vendor is increasingly evident with the formation of a structured international sales department and their active participation in various specialized professional exhibitions at the global level.[175]

Pegasus demonstrates how the unregulated spyware market facilitates mass human rights violations. This phenomenon has reached a more alarming level with AI-based targeting systems like Lavender and The Gospel, which are expanding the scale of repression through algorithmic control. Addressing these

[174] Ní Aoláin, *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach.*
[175] Arquillière et al., *Predators for Hire: A Global Overview of Commercial Surveillance Vendors.*

challenges requires international oversight, corporate accountability, and stronger legal protections to prevent the uncontrolled proliferation of spyware and its role in reshaping global security and power structures.[176]

David Lyon offers a comprehensive assessment of surveillance as a social phenomenon. Originally understood as a tool of state power, surveillance has now undergone a transformation and transfiguration into a complex commercial instrument. According to Lyon, surveillance is "the focused, systematic, and routine attention to personal details for the purpose of influencing, managing, protecting, or directing."[177] Through his thinking, Lyon demonstrates that surveillance's primary strength lies in its power dynamics, which enable it to operate as both a means of social control and an instrument of state power.

The case study of Pegasus's use illustrates the convergence of privatization, transnationalization, and digitalization in modern surveillance. This phenomenon reveals the interconnectedness of technology and monitoring practices across various sectors, involving government intelligence agencies, private companies, and even authoritarian regimes. This integration demonstrates that surveillance no longer operates independently but rather through a global ecosystem that transcends national sovereignty.[178] This situation underscores the urgency of establishing a policy framework that regulates the sale and export of spyware technology by integrating human rights considerations into cyber surveillance governance. This regulatory reform is crucial to ensure the protection of civilians from the destructive consequences of the misuse of such technology by both state actors and the private sector.[179] Furthermore, the UN Special Rapporteur on Freedom of Opinion and Expression has emphasized that the global export

[176] Afrose, "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine."
[177] Quoted from Cecile Lourens , "Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware," *Diggit Magazine,* 20 May 2022, https://www.diggitmagazine.com/articles/surveillance-intersection-technology-business-and-politics-case-study-pegasus-spyware . Accessed on 12 January 2026
[178] Lourens, "Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware."
[179] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

control framework, as well as national implementations in regions where the NSO Group operates, are inadequate in regulating surveillance technology and mitigating its impact on human rights. This situation poses a serious risk of fundamental rights violations, particularly in jurisdictions with minimal or no legal frameworks regarding the use of such spyware.[180]

This gap between export regulations and on-the-ground practice is starkly reflected in the case of Azerbaijan. Although the country is not on the official list of NSO Group licensees, the strong indication of its presence there is a cause for concern. If NSO Group is proven to have sold cyber surveillance licenses to government agencies in Azerbaijan, a country with a track record of civil liberties violations, political repression, and torture, it would expose the fact that no one can be certain how far Pegasus's reach is facilitating repression in unmonitored regions.[181]

In recent decades, the need to regulate and monitor the development and distribution of cyber surveillance technology has been accepted worldwide. This technology is categorized as dual- use technology from an international legal perspective because it can be used for both civilian and defense purposes. The export of dual-use technology is regulated in many countries through the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. This agreement is designed to promote transparency and accountability in the international transfer of arms and sensitive technology. The Wassenaar multilateral export control regime facilitates the exchange of information among participating countries and aims to improve the oversight of arms and dual-use exports. The main instrument used by the Wassenaar Agreement to achieve this goal includes a list of goods subject to export controls by participating countries.[182]

---

[180] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[181] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[182] Although the Wassenaar Agreement is not legally binding, governments that adopt the Wassenaar Agreement control list generally incorporate it into domestic law and require those exporting listed goods to

The Wassenaar Agreement is a key component of the multilateral export control system, containing separate regulations for weapons of mass destruction and their delivery systems. The agreement focuses on multilateral efforts to control the proliferation of conventional weapons and dual-purpose weapons by harmonizing and coordinating each country's export control policies. The agreement only targets the transfer of specific items, not their development, production, possession, or use. The agreement has two control lists: the Munitions List, which includes conventional weaponry, and the List of Dual-Use Goods and Technologies. The control list is regularly reviewed and updated, and any decisions regarding listed goods are made by consensus.[183] Thus, the controls adopted by the Wassenaar Agreement can play a key role in improving oversight, transparency, and restrictions on trade in spyware and other cyber surveillance tools.[184] Once a member decides to include a particular good on one of its control lists, implementation is left to the participating countries. Changes must be implemented and applied at the national level to be effective, and considerable flexibility is given to individual countries.[185] The implementation of the Wassenaar Agreement in practice can be seen in the following table.[186]

obtain export permits prior to export, taking into account factors such as the policies and security levels of the destination country. See Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[183] Elaine Korzak, "Regulating Commercial Spyware Through Export Controls," *Lawfare,* 10 December 2025, https://www.lawfaremedia.org/article/regulating-commercial-spyware-through-export-controls . Accessed on 20 January 2026

[184] Bromley and Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint.*

[185] As of 2025, Wassenaar membership includes 42 countries, primarily member states of the Organisation for Economic Co-operation and Development (OECD), as well as Ukraine, the Russian Federation, and India. While this includes most major industrialized countries and leaders in technological innovation, the arrangement currently excludes a number of important countries, such as Israel and China. See Bromley and Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint.*

[186] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

Region/Country	Description
European Union 	• The EU implements a regime of authorization and approval of exports of certain dual-use products through the European Regulations for the Export of Dual-Use Products. • The Regulation covers export controls for intrusion software and communications surveillance systems. According to the Regulation, when EU Member State authorities consider whether to approve or reject an export application, they must take into account, among other things, the Member State's obligations under sanctions imposed by the Council of Europe or the UN Security Council, and considerations relating to the end use of the exported goods. • In addition, the enhanced Export Control Regulations that came into force in the European Union in September last year explicitly require all exports to respect, and comply with, human rights and humanitarian law.

 United States of America	• The Bureau of Industry and Security (BIS), part of the United States Department of Commerce, is responsible for regulating the export of dual-use products in the United States. The agency operates: (1) a licensing system for the export of controlled products; (2) determines export policy for controlled products; and (3) implements enforcement policy and carries out extraterritorial enforcement. • In December 2021, the Biden administration acknowledged the ongoing threat posed by cyber surveillance technology and announced the United States would combat the use of cyber espionage and surveillance technology to spy on dissidents and human rights activists worldwide and place human rights at the center of United States foreign policy; • As part of this effort, the BIS End-User Review Committee decided to add four foreign entities, including two Israeli companies, NSO Group and Candiru, to the Entity List. The US Export Administration Regulations (EAR) subsequently imposed additional licensing requirements for exports to the listed entities and limited exemptions for exports, re-exports, and transfers to those entities.[187]

[187] However, it is unclear whether adding companies to the Entity List has prevented the sale *of spyware,* and there may be a need for stricter oversight of the cyber surveillance industry, whose end users and end uses are notoriously difficult to track and whose abuse is difficult to combat. These considerations led the BIS in May of last year to issue revised export regulations that impose new controls on cybersecurity items that could be used for espionage or other actions that disrupt the network or device on which they are located.

The application of the Wassenaar Agreement in the context of two main jurisdictions, namely the European Union and the United States, provides several reflections that can be taken as lessons:[188]

First, export control decisions have been complicated by the need to balance new and complementary interests. In addition to economic interests and national security concerns, countries need to consider human rights and cybersecurity considerations within the context of export controls. These multiple considerations require each country to juggle its own priorities to effectively engage with and shape export controls and other international regulatory efforts.

Second, the Wassenaar export controls are controversial and have long-term implications for the Wassenaar Agreement and its members. The usefulness of export controls hinders international progress on this issue. Rather than focusing on a single regulatory mechanism, stakeholders should pursue a range of national and international measures to address commercial spyware.

Third, there are inherent limitations to the Wassenaar controls and export controls in general that need to be identified and acknowledged. Furthermore, the Wassenaar controls only target a small subset of commercial spyware technologies. This will limit the effectiveness of export controls.

Based on these reflections, the broad discretion of participating countries in implementing the Wassenaar Agreement becomes a critical point and gap in the effectiveness of restrictions on commercial spyware exports.[189] On the other hand, Israel, which dominates the global spyware market, is increasingly not responsible for spyware exports because Israel is not a signatory to the Wassenaar Agreement. Israel claims to use a control list and enforce this agreement through national laws, specifically the Israeli Defense Export Control Law of 2007. This law demonstrates Israel's compliance with the provisions of the

---

See Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

[188] Korzak, "Regulating Commercial Spyware Through Export Controls."

[189] Doron Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach," *Lawfare,* 12 February 2016, https://www.lawfaremedia.org/article/can-export-controls-tame-cyber-technology-israeli-approach . Accessed on 25 January 2026.

Wassenaar Agreement that allow for the removal of trade barriers for dual-purpose goods. The law regulates the export of defense and dual-purpose equipment, services, and know-how, includes requirements for obtaining export permits from competent authorities, and establishes obligations for permit holders, such as inspection, record-keeping, and reporting responsibilities.[190]

While Israel strictly monitors the export of defense and dual-purpose technologies such as spyware, its controls are primarily based on defense, national security, and foreign relations considerations. These considerations ignore the human rights implications of these technologies. Even if human rights were considered by regulators, the promotion of Israel's national security policy would likely take precedence over human rights protection. Government decisions regarding defense export licenses are not subject to judicial review. This was reinforced by a precedent-setting 2022 ruling by the Israeli Supreme Court, which ruled that exporting offensive cybertechnology to foreign countries falls outside the courts' jurisdiction. Regulation of such technology is considered the government's prerogative, with national security considerations being the primary priority. This ruling effectively closed legal avenues for civilians and humanitarian organizations to challenge defense exports to dictatorships or repressive regimes.[191]

In line with this, Anna W. Chan emphasized the importance of implementing a shared responsibility regime in the mechanism of spyware sales by multinational corporations. Building on the Wassenaar Agreement as the main international instrument for controlling the transfer of arms and surveillance technology, this regime requires states to actively monitor corporations closely. This not only aims to prevent human rights violations from the outset but also to provide victims with broader access to justice and legal accountability. Furthermore, the international legal system has allowed for various

[190] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."
[191] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

conceptualizations of shared responsibility.[192] A parallel partnership between states and multinational corporations aims to bridge the accountability gap regarding the behavior of multinational corporations. This is based on the principle that if a corporation acts on the instructions or under the direction or control of a state, its behavior can be attributed to the state. Furthermore, this shared responsibility involving non-state actors can arise in specific situations through institutional arrangements, where states contract with corporations to carry out specific surveillance activities.[193]

The application of this shared responsibility can be referred to the Draft Articles on Responsibility of States for Internationally Wrongful Acts prepared by the International Law Commission. These draft articles only apply to private corporate entities if their behavior is attributed to the state through the necessary relationship between the corporation and the state. The Draft Articles aim to codify the basic rules of international law regarding state responsibility by establishing the legal requirements for determining when a state is considered responsible for internationally wrongful acts, whether in the form of active action or omission, and determining the legal consequences arising from them. The general rule is constructed through the linkage of the behavior of a state at the international level with the behavior of its governmental organs, or other parties who have acted under the direction, instigation, or control of those organs.[194]

A similar normative construct can be found in the United Nations Guiding Principles on Business and Human Rights. Principle 4 specifically states that:

"States must take additional steps to protect against human rights abuses

[192] This shared responsibility regime will build on the multi-stakeholder regime established by the Code of Conduct for Private Security Service Providers (ICoC). The implementation of this code is overseen by the International Code of Conduct Association (ICoCA), which acts as an oversight committee. This committee consists of representatives from companies, civil society groups, and governments. Through collaboration, the shared responsibility regime will provide better monitoring, reporting, and certification practices for corporate entities. See Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

[193] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

[194] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

by business enterprises that are owned or controlled by the state, or that receive substantial support and services from state institutions."

Principle 5 stipulates that states do not absolve their obligations when they privatize the provision of services to businesses that may impact human rights. On the other hand, Principle 11 stipulates that companies must avoid violating the human rights of others and address adverse human rights impacts, including taking adequate measures for prevention, mitigation, and, where necessary, providing redress. Some operational due diligence mechanisms proposed by the UN Guiding Principles include adopting a statement of commitment to human rights, adapting risk management systems to mitigate actual impacts, and tracking the implementation of human rights policies.[195]

Over time, several countries and private sectors have developed various initiatives to address the proliferation and misuse of spyware and other cyber surveillance tools. These initiatives aim to establish new norms and standards, encourage more effective implementation of international human rights law, and seek financial compensation from spyware manufacturers. Export controls and sanctions are essential components of broader efforts to regulate the production, trade, and use of spyware and other cyber surveillance tools. Since 2012, five categories of spyware and other cyber surveillance tools have been added to the dual-purpose device control list managed by the Wassenaar Agreement and the European Union. Furthermore, the European Union adopted a new version of the EU dual-use products regulation in 2021, which aims to strengthen controls on the export of spyware and other cyber surveillance tools. The EU sanctions regime includes a ban on the export of surveillance technology to certain recipients, while US sanctions specifically target spyware manufacturers. Similarly, 43 countries have committed to implementing export controls to prevent the transfer of spyware and other cyber surveillance tools that risk facilitating violations of human rights and international humanitarian law. This commitment is particularly significant because these countries are the base of operations for 68

[195] Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

percent of the companies producing spyware and cyber technology worldwide.[196]

In general, there are three ways to address the spread and misuse of spyware technology by government regimes worldwide. *First*, focusing on strengthening national export control regimes integrated with human rights standards. This approach could be realized through the creation of new legally binding international agreements, including the imposition of strict sanctions for misuse of such technology. *Second*, emphasising the responsibility of cyber surveillance corporations to conduct due diligence and independently monitor the use of their technology. The success of this mechanism depends heavily on the risk of business losses or negative reputational impacts arising from persistent associations of their technology with human rights violations.

The *third* solution involves regulatory mechanisms by private companies directly harmed by the misuse of spyware technology. In this approach, large technology companies whose digital ecosystems have been infiltrated take independent action to limit the scope of spyware manufacturers, for example through lawsuits, blocking technical access, and proactively strengthening security systems to protect their users.[197]

These private regulatory mechanisms continue to evolve in response to the emergence of offensive cyber capabilities that exploit vulnerabilities in the products of tech giants. These exploits are used to break into and take over users' devices worldwide, directly compromising the integrity of their systems. This phenomenon has prompted major tech companies like MetaTrader, Amazon and Apple to take the initiative to fill the regulatory vacuum left by export control regimes. Through these private regulatory mechanisms, they implement decisive action to hinder the movement of companies commercializing these hacking capabilities.[198]

---

[196] Bromley and Maletta, *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint.*
[197] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."
[198] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

The implementation of this mechanism is evident in a series of decisive actions taken by tech giants. In 2019, Facebook (now Meta) sued NSO Group for exploiting a security flaw in the WhatsApp app to install malware. Apple followed suit, demanding a permanent ban from using Apple products and services following the discovery of hacking of iPhone users globally. In addition to litigation, preventive measures are also being taken technically. In late 2021, Meta closed hundreds of accounts affiliated with an Israeli cyberintelligence firm after being detected spying on activists, politicians, and journalists in various countries. Amazon took similar action by cutting off access to its cloud services, which were misused by NSO Group to spread malware. These cases confirm that large tech companies can act as private law enforcement actors by cutting off access to their product ecosystems. This action is part of a soft transnational enforcement mechanism, a transnational enforcement mechanism that operates beyond national sovereignty. Through this global network, private companies indirectly help uphold international standards and protect cybersecurity and human rights globally.[199]

On the other hand, the state-centric doctrine of international human rights law has created a number of problems for lawyers seeking to hold corporations accountable for human rights violations. Under the state-centric doctrine, corporations are neither subject to treaty obligations nor are they primary actors under international law. This doctrine leaves corporate victims seeking redress in their home country's judicial system facing numerous obstacles.[200]

---

[199] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

[200] Human rights lawsuits under the Alien Tort Statute were initially often described as the primary engine for transnational human rights litigation in the United States. However, the United States Supreme Court's ruling in Kiobel v. Royal Dutch Petroleum Co. later reduced the utility of litigation using the Alien Tort Statute. The Supreme Court in the Kiobel case unanimously ruled that the petitioners' claims fell outside the jurisdiction of the Alien Tort Statute because the Alien Tort Statute does not apply extraterritorially if the claim does not touch and concern the United States with sufficient force. Thus, this claim can no longer be used to hold multinational corporations legally liable for human rights violations. Even when a remedy is available in a national legal system, a number of other issues can make seeking redress in that national legal system less attractive; for example, the principle that corporations maintain separate legal personality can complicate the legal liability of a parent company for the actions of its subsidiaries because each is a separate legal entity. Moreover, a legal system such as the United States, where the doctrine of forum non conveniens applies, may

The emergence of various regulatory models outside the state framework is now beginning to erode traditional doctrines of international law. While previously the state was considered the primary duty bearer for enforcing human rights standards and controlling the export of surveillance technology, this role is now shifting.[201]

However, relying on self regulation initiated by tech giants is not an ideal solution. The fundamental problem lies in a conflict of interest. The motivations driving these companies to act often differ from those of the state, as well as from those of the primary victims of cyber surveillance systems. Tech companies do not consider the public or national interest when pursuing private regulation. Instead, they choose to speak out and act only when they experience financial losses, or when they draw attention to ways to address misuse of their products in a financially profitable manner. Similarly, a private regulatory framework should not only place compliance responsibilities on private companies, but also should not rely on private bodies, whose primary goal is to maximize profits rather than uphold the rule of law and human rights.[202]

David Kaye and Sarah McKune state that the use of spyware is a complex issue because it attacks individual privacy, due process, and freedom of expression and association. Therefore, an appropriate legal framework must be based on international human rights law, which requires: (1) a legitimate interest in any interference with fundamental rights and peaceful demonstration; (2) legality; and (3) necessity and proportionality. Based on this principle, countries that use surveillance devices must do so based on a legitimate interest in

---

prevent a case from proceeding when another jurisdiction is more appropriate or convenient, such as the location where the alleged tortious act resulting in the human rights violation occurred. See, Ruth Cowley, "Kiobel's Impact on Disputes in International Law," *Norton Rose Fulbright,* May 2013, https://www.nortonrosefulbright.com/en/knowledge/publications/ 94bc936c/kiobels-impact-on-disputes-in-international-law . Accessed on 25 January 2026. See also, Chan, "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware."

[201] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

[202] Zvi, "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading."

national security or public order. However, the existence of such an interest is only one aspect of the legal investigation. The requirement of legality means that the use of spyware must be regulated by specific law and accompanied by strict safeguards to eliminate the risk of arbitrary interference. Necessity and proportionality require that such interference must be the least intrusive instrument among those that might achieve a legitimate aim and be proportionate to the aim sought.[203]

In terms of legality, the use of spyware must establish clear human rights boundaries, given that this technology allows for unhindered remote access to all device contents and real-time control of audio, video, and location functions. However, to date, neither the industry nor its users have been able to formulate legal standards or practices that address this significant challenge. Given the widespread track record of human rights violations, it's hard not to assume that truly stringent legal boundaries would simply destroy this industry's highly profitable business model. It's no surprise, then, that the spyware industry is reluctant to propose serious regulations.[204]

At the same time, the burden of proof for the necessity and proportionality test should rest with industry and user states. They must be able to demonstrate that no other law enforcement instruments are available, including conventional surveillance practices that do not require remote penetration of personal devices. However, this principle is difficult to enforce due to the lack of government transparency regarding the strategic interests at stake. So far, much of the evidence suggests the opposite; spyware use is rarely linked to preventing serious crimes, but rather to exposing human rights violations, as documented by Citizen Lab, Amnesty International, and Access Now. This lack of proof is also closely related to the issue of extraterritorial jurisdiction. Often, states use spyware to hack targets outside their borders without authorization. Legally, the need for cross-border data should trigger the use of Mutual Legal Assistance Treaties. The

[203] David Kaye and Sarah McKune, "The Scourge of Commercial Spyware—and How to Stop It," *Lawfare,* 25 August 2023, https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it . Accessed on 23 February 2026

[204] Kaye and McKune, "The Scourge of Commercial Spyware—and How to Stop It."

use of MLATs ensures judicial oversight and the right to due process, precisely the very thing spyware is deliberately avoiding. Similarly, Fionnuala Ní Aoláin, the UN Special Rapporteur on counter-terrorism and human rights, asserted that because this technology inherently lacks auditability and transparency, it will never be able to meet human rights standards, no matter how stringent regulations are implemented.[205]

The UN Special Rapporteur on Counter-Terrorism and Human Rights' Position Paper sets out a number of minimum technical requirements that must be met for spyware to comply with human rights standards. These requirements include:[206]

1) Allowing users to specifically target certain data and metadata, rather than automatically monitoring and recording all data and metadata;

2) Avoiding automated access to data relating to the contacts of targeted individuals, unless the user specifically requires such additional information for investigative purposes;

3) Designing mechanisms to prevent malicious use, such as tagging systems and 'kill switches' in cases of apparent misuse; and, in any event;

4) Creating an irremovable, permanent, and uneditable audit record of what actions have been taken by the user of the spyware, including any data/metadata tampering/modification, when it occurred, and by whom it was done so that the use of the tool can be verified, and its compliance with human rights assessed after the fact by a judicial authority. Part of that irremovable and uneditable record should be some form of identifier or watermark so that the judicial authority overseeing the complaint can verify the manufacturer of the spyware alleged to have been used against the victim and the customer to

[205] Kaye and McKune, "The Scourge of Commercial Spyware—and How to Stop It."
[206] Ní Aoláin, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism.*

whom the spyware was originally supplied and, from that source, can compel disclosure of the audit record so that the legality of any complained-of use can be adequately reviewed.

Kaye and McKune emphasized that the moratorium remains a crucial temporary measure amidst widespread spyware abuse and global intimidation. In addition to the moratorium, other strategic efforts include investigative reporting by human rights organizations and journalists, the active involvement of UN experts, and lawsuits filed by victims and corporate actors such as WhatsApp and Apple. Legislative investigations, government blacklisting, and multilateral dialogue are also crucial tools in building a global accountability regime to ensure that all countries adhere to human rights standards. Furthermore, transparency, oversight, and government accountability, along with effective pathways for redress, must be part of the regulatory ecosystem, both nationally and internationally. At the same time, private sector involvement in the trade in surveillance technology must be ended or at least strictly limited.[207]

H. Challenges in Resolving Cases for Spyware Victims: Limitations of Existing Human Rights Protections in Providing Protection of Emerging Digital Rights

Legal remedies pursued by victims of commercial spyware face serious structural barriers, in all dimensions of jurisdiction, evidentiary challenges, and the physical safety of the plaintiffs themselves. One of the most dramatic illustrations of these non-litigation barriers is the case of Ahmed Mansoor, an internationally recognized human rights activist from the United Arab Emirates and recipient of the Martin Ennals Award. In August 2016, Mansoor received an SMS message on his iPhone promising "new secrets" about detainees being tortured in UAE prisons. When he forwarded the message to Citizen Lab researchers, the link was identified as part of an exploitation infrastructure linked

[207] Kaye and McKune, "The Scourge of Commercial Spyware—and How to Stop It."

to the NSO Group and its Pegasus spyware.[208]

In March 2017, Mansoor was arrested at his home by twelve members of the UAE state security apparatus, and after spending much of his detention in complete isolation with very limited access to family and legal counsel, he was sentenced to ten years in prison in May 2018 on charges of using social media to spread "false information and rumors that undermine national unity." Mansoor's case illustrates how a potential victim of digital surveillance can be removed from the legal system of the same state that allegedly carried out the surveillance, leaving him with no access to justice at all.

In formal litigation, jurisdictional hurdles often prove insurmountable. In a lawsuit filed by Hanan Elatr Khashoggi, the wife of murdered journalist Jamal Khashoggi, against NSO Group before the United States District Court for the Eastern District of Virginia, the court granted NSO Group's motion to dismiss the lawsuit on the grounds of lack of personal jurisdiction. The court concluded that the plaintiffs had not sufficiently demonstrated NSO Group's direct involvement specifically within the state of Virginia, given that the disputed surveillance was conducted by third-party actors, namely the governments of Saudi Arabia and the United Arab Emirates. This ruling was subsequently affirmed by the Fourth Circuit Court of Appeals, which affirmed that NSO Group did not intentionally exploit the privilege in conducting its activities in Virginia. This jurisprudence confirms that the "purposeful availment" doctrine in United States personal jurisdiction law structurally disadvantages victims when spyware developers operate indirectly through government clients.[209]

In Southeast Asia, the case of Jatupat Boonpattararaksa in Thailand illustrates a different evidentiary obstacle. The human rights activist sued NSO Group after his devices were infected with Pegasus three times between June and

[208] Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against A UAE Human Rights Defender," *The Citizen Lab,* August 24, 2016, https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/ .

[209] *Hanan Elatr Khashoggi v. NSO Group Technologies Limited, et al.,* No. 23-2234 (United States Court of Appeals for the Fourth Circuit, May 21, 2025), https://law.justia.com/cases/federal/appellate-courts/ca4/23-2234/23-2234-2025-05-21.html .

July 2021, seeking 2,500,000 Thai Baht (equivalent to US$72,129) in damages, a cease and desist of the use of the spyware on his devices, and access to and deletion of the extracted data. However, the court dismissed the lawsuit, citing insufficient evidence, particularly the inadequate description of the forensic investigation process and results that led to the conclusion that the plaintiff's devices had been infected with the spyware. This ruling drew criticism from Amnesty International, which stated that the court's failure to acknowledge NSO Group's role in facilitating human rights violations was deeply concerning.

Technically, Amnesty International and Security Lab have conducted in-depth forensic analyses of devices belonging to human rights defenders in Thailand and found evidence of Pegasus infection, but the court's evidentiary standard proved beyond what plaintiffs could meet on their own at trial. This evidentiary barrier is compounded by NSO Group's consistent position that it is merely a software developer with no control over how it is used, and that its products are sold exclusively to government agencies for law enforcement and counterterrorism purposes—a claim that contradicts civil society research documenting the systematic abuse of journalists and activists around the world. Taken together, these three dimensions of impunity—pre-suit arrest, lack of jurisdiction, and high forensic evidentiary standards—form a multi-layered structure of impunity that effectively denies victims of commercial spyware access to justice.[210]

Meanwhile, the claim that digital rights are becoming human rights is not free from controversy because each country and judicial institution can interpret them differently.[211] This difference is also demonstrated by the fact that the fundamental dimension of personal data protection is still being debated, particularly within the European Union. The issue of the fundamentality of data

[210] Amnesty International, "Thailand: Dismissal of Landmark Case a Critical and Alarming Setback in Fight Against Unlawful Use of Spyware," 21 November 2024, https://www.amnesty.org/en/latest/news/2024/11/thailand-dismissal-of-landmark-case-a-critical-and-alarming-setback-in-fight-against-unlawful-use-of-spyware/ .

[211] Yuval Shany, From digital rights to international human rights: The emerging right to a human decision maker, Accessed on 4 May 2026

protection is important because it has been separated from the right to privacy in European Union legislation and has been referred to as a fundamental right. The Charter of Fundamental Rights of the European Union articulates the right to privacy for citizens in Article 7 and the right to data protection in Article 8. Article 7 of the Charter establishes provisions on respect for private and family life, covering a wide range of issues, from private and family life to home immunity and the confidentiality of communications. This provision is dedicated as a special article to the protection of personal data so that it can be treated appropriately. Meanwhile, Article 8 of the Charter recognizes the right to personal data protection as a new fundamental right that is distinct from the rights to respect for private and family life, home, and communications listed in Article 7 of the Charter. Article 8 of the Charter is inspired and based on various legal instruments, although the protection of personal data is not recognized as a specific right within the framework of existing international instruments on the protection of human rights. Article 8 of the European Convention on Human Rights, including the jurisprudence of the European Court of Human Rights, on the protection of privacy and private life, inspires the fundamentality of the protection of personal data, although the protection of personal data is not explicitly mentioned in the European Convention on Human Rights.[212]

On the one hand, there are data protection rules and cases that qualify as fundamental. For example, provisions in the General Data Protection Regulation concerning the processing of sensitive personal data, such as that revealing a person's sexual or political orientation, medical condition, or race (ethnicity), qualify as fundamental and important rights in a democratic society. Furthermore, certain cases in the jurisprudence of the Court of Justice of the European Union articulate the crucial issues for securing human rights protection. For example, the Digital Rights Ireland case concerned the legality of the Data Retention Directive, which obliges states to monitor and store the internet traffic data of millions of innocent citizens. The Court of Justice determined that the Data

[212] Bart van der SlootLegal Fundamentalism: Is Data Protection Really a Fundamental Right? In Ronald Leenes, et al. , *Data Protection and Privacy: (In)visibilities and Infrastructures*, (Cham: Springer International Publishing AG, 2017)

Retention Directive did not establish clear and precise rules governing the extent of interference with the fundamental rights enshrined in Articles 7 and 8 of the European Charter of Human Rights. There are also other factors that appear to indicate that data protection appears to protect values that differ significantly from those protected by conventional human rights. Based on the EU Directives and Regulations, data protection rules aim to protect two very opposing values, namely the interests of individuals to protect their personal data on the one hand and the interests of data controllers to process their data in the EU internal market on the other.[213]

This normative question can be drawn from the nature of data protection regulations and cases by the European Court of Human Rights. Human rights conventionally protect only a strictly limited number of values considered essential to personal liberty. The jurisprudence of the European Court of Human Rights, for example, is based on concepts such as the *ratione personae*, *ratione materiae*, and the *de minimis* rule. Under this principle, interests that have a serious impact on the life and privacy of the plaintiff are protected within the scope of the Convention. Consequently, the processing of personal data would not be protected within the scope of Article 8 of the European Convention on Human Rights if it concerns the processing of trivial data, such as names and addresses, or when the data processing activity should be considered an ordinary, everyday activity. Article 8 of the European Convention on Human Rights stipulates the protection of privacy and private life, although the protection of personal data is not explicitly included within its scope. Therefore, there is a threshold for cases to fall within the scope of human rights protection. Data protection instruments, on the other hand, do not aim to protect a minimum number of essential personal values. On the contrary, the scope of personal data has been significantly expanded over time. As long as the data can be used to identify a person, it falls within the scope of personal data protection.[214]

This demonstrates a fundamental difference in the nature of human rights

[213] Ibid.
[214] Ibid.

and personal data protection regulations. Human rights provisions are based on absolute and conditional prohibitions. States may not restrict the rights to privacy and freedom of expression unless this is necessary in a democratic society and is regulated by law. The right to privacy protects individuals against government interference, while data protection regulations already represent a compromise between the rights and interests of data subjects and data controllers. Data protection regulations themselves represent a compromise between the free flow of information and the protection of personal data. For the most part, data protection regulations concern procedural aspects and the quality of personal data processing. For example, when personal data is processed, data controllers must ensure that the data is accurate and up-to-date, that it is processed securely and confidentially, and that the processing is transparent. Article 8 of the Charter not only stipulates that individuals' personal data must be protected but also specifies when and how personal data can be lawfully processed. Furthermore, not only does a general limitation clause apply to Article 8 of the Charter; the fundamental right to data protection itself represents a compromise between various legitimate interests. Thus, while the right to privacy protects individual interests and can be limited under certain circumstances, for example, if the interests of others or the wider community outweigh those of the individual, the right to data protection itself is a compromise between various interests, including the interests of businesses and states in processing data. In this respect, data protection appears to differ fundamentally from human rights. A key assumption underlying the right to data protection is that data processing itself is legitimate and even necessary for businesses and states, and that even citizens need to process their personal data.[215] Meanwhile, there is an assumption that the processing of sensitive personal data and other data that significantly impacts an individual's interests is already protected under the human rights framework, namely under the right to privacy. The same can be said for mass surveillance, data storage, and large-scale wiretapping; these actions typically constitute violations of the confidentiality of communications and the right to private life.

[215] Ibid.

Therefore, removing the right to data protection from the fundamental rights framework would not leave these interests unprotected.[216]

The different interpretations of the right to personal data protection, which falls within the scope of digital rights, and conventional human rights, are inseparable from the different perspectives of international human rights law theory and practice, which boil down to three specific characteristics of human rights: universality, inalienability, and state obligations. Rights recognized under international human rights law are inherent to every human being, and their availability is independent of status or behavior and, consequently, inalienable. Although human rights are, in principle, non-absolute and can be limited to protect the rights of others or important public interests, human rights create obligations for states exercising jurisdiction over the relevant individual rights holders. In the context of digital human rights, this implies an obligation to protect individuals from violations of their rights by other individuals or companies, including technology companies. Furthermore, according to Yuval Shany, the shift from digital rights to human rights tends to be based on a specific pattern of justification, consisting of moral claims and considerations supporting the universality of the right, its inalienability, and the imposition of correlative obligations, an analysis of the problem involving a cost-benefit analysis supporting the recognition of the right, and the identification of broad political support for recognizing the right in question as a new human right. [217]

At the same time, the disruptive impact of artificial intelligence systems could place significant pressure on existing human rights. Furthermore, the black-box nature of artificial intelligence systems and the resulting lack of transparency surrounding algorithmic decision-making processes call for consideration of whether existing human rights norms should be revised. This revision of existing human rights is necessary to enable them to capture the new human needs and interests posed by these new technologies. To what extent are existing human rights laws adequate to address the challenges posed by the

[216] Ibid.
[217] Yuval Shany, op.cit

increasing use of artificial intelligence systems, and to what extent do they need to be revised to effectively address the new challenges posed by the increasing application of these systems?[218]

Advances in the application of artificial intelligence technology have paved the way for innovative applications in neuroscience, particularly in neural signal processing and neurotechnology. Artificial intelligence technologies, including machine learning, deep learning, and data analytics, have revolutionized neural signal processing by improving the accuracy, speed, and efficiency of data analysis. The integration of artificial intelligence with neurotechnology has also opened new doors for the development of assistive technologies. brain-computer interfaces, neuromodulation techniques, and neuroprosthetics. Artificial intelligence algorithms can enhance the performance and adaptability of these devices, enabling precise control, interpretation, and translation of neural signals into actionable commands or feedback.[219]

Other technological developments based on artificial intelligence, such as neurotechnology, still require large amounts of data for their operations. At the same time, nearly all publicly available internet data have been analyzed by large artificial intelligence companies. These companies now need new data to continuously refine the new innovation models they are designing. In this context, neurotechnology presents an exciting opportunity for these companies, as it allows them to collect massive amounts of brain data. This brain-sourced data is incredibly rich in information. Many companies will capitalize on this opportunity. A further consequence is that mind surveillance will become increasingly widespread and invasive. This situation poses various risks because these neural sensors can also modify brain activity.[220] Neurotechnology will gradually be embedded in many consumer devices, and thus will impact the lives

[218] Yuval Shany, The Need for and Feasibility of an International AI Bill of Human Rights, Accelerator Fellowship Programme, Institute for Ethics in AI, University of Oxford November, White Paper, 2025

[219] Siamak Pedrammehr, et.al ., (eds.), Artificial Intelligence Advancements in Neural Signal Processing and Neurotechnology, https://www.frontiersin.org/research-topics/61562/artificial-intelligence-advancements-in-neural-signal-processing-and-neurotechnology , Accessed on 4 May 2026

[220] Arnaud Mittempergher, Artificial intelligence can read our thoughts, 2025, see https://www.artificialreality.ch/p/ai-can-read-our-thoughts , Accessed on 30 April 2026

of many people. Arnaud Mittempergher identifies the risks of utilizing neurotechnology:[221]

1) Mass surveillance by government and private parties;
2) Loss of privacy;
3) Mental surveillance in the workplace;
4) Surveillance of political dissidents;
5) Manipulation of thought for political purposes;
6) Thought police;
7) Forced interrogation;
8) Manipulation of brain processes that can influence a person's intentions, emotions, and decision-making;
9) Manipulation of perception and memory;
10) The insertion of artificial images into a person's mind;
11) Risks to mental integrity, human dignity, personal identity, freedom of thought, and autonomy;
12) Cyberattacks on brain implants can have a variety of consequences, including memory theft, modification, or deletion. These attacks can also affect a person's physical autonomy or cause significant psychological impacts, such as anxiety, depression, or other mental health issues;
13) Discrimination by insurance companies;
14) Manipulation of consumers by commercial companies;
15) The creation of weapons designed to paralyze and disorient the human brain;

[221] Arnaud Mittempergher, Neurorights against mental surveillance, 2025, see https://www.artificialreality.ch/p/neurorights-against-mental-surveillance , Accessed on 1 May 2026

16) Sale of brain data to third parties.

In this context, the UN in 2024 raised concerns about the use of neurotechnology by exploiting the absence or weakness of legal instruments that could impact human rights:[222]

It is likely that in the coming years, neurotechnology products with inadequate safety measures and human rights risks will be widely commercialized. These products will permeate every aspect of daily life, despite the fact that in most countries, applicable legal instruments are unclear, weak, or even non-existent. Loopholes in legal instruments, lack of technical expertise and capacity, and the absence of adequate regulatory bodies are factors that large, profit-driven companies will undoubtedly exploit. The risk is that, without the necessary safeguards in place, the industry will continue to grow unchecked in the same direction: prioritizing profitability and convenience over ethical and human rights considerations.

Marcello Ienca and Roberto Andorno believe that existing rights are no longer adequate to address the risks associated with neurotechnology. Therefore, there is an urgent need to reconceptualize certain human rights, or even create new rights. Ienca and Andorno then coined the term *neurorights* to address the inadequacy of existing human rights in addressing the risks posed by neurotechnology.[223] They emphasize the *terra incognita* situation of international human rights law in addressing the threats posed by neurotechnology to various human rights. Therefore, human rights law must immediately reform and adapt to the risks arising from the application of this technology:[224]

Although neurotechnology has the potential to impact human rights, such as privacy, freedom of thought, the right to mental integrity, freedom from

[222] Ibid.
[223] Ibid.
[224] Marcello Ienca and Roberto Andorno, Towards new human rights in the age of neuroscience and neurotechnology, Life Sciences, Society and Policy, 13:5 (2017)

discrimination, the right to a fair trial, or the principle of non-self-incrimination, international human rights law does not yet contain any explicit reference to neuroscience. Unlike other biomedical developments that have been the subject of standard-setting efforts at both the domestic and international levels, neurotechnology remains largely terra incognita for human rights law. Nevertheless, the implications of neuroscience and neurotechnology for inherent human characteristics demand a swift and adaptive response from human rights law.

The use of surveillance technology has the potential to threaten new human rights emerging in the online realm. The emergence of new human rights is triggered by the use of new technological devices. This requires new protections to adapt to the manifestations of these new human rights violations. Recognition of the inadequacy of protection for certain groups compared to others justifies the urgency of new human rights protections. Another argument is that new contemporary conditions challenge the ability of established human rights to provide adequate protection for important social values. The articulation of these new human rights is inseparable from the contestation between conventional human rights and new human rights. This contestation gives rise to the inability of existing human rights protections. In this context, the issue of equal protection of human rights in the online realm with that in the offline realm arises. At the same point, the issue of the concept of protection that is entirely rooted in and derived from the offline realm or the effective application of rights restoration efforts that apply in the offline realm to the online realm arises.[225]

The emergence of new human rights has influenced the conventional vertical human rights governance model, at least partially losing its effectiveness in addressing the issues of human rights interactions with digital technology. The inconsistency between offline human rights governance frameworks and models and cyber reality has gradually transformed into discursive justification for new governance models. The horizontal governance model is proposed as a more

[225] Mart Susi, *The Non-coherence Theory of Digital Human Rights*, (Cambridge: Cambridge University Press, 2024)

appropriate model for application in the context of human rights interactions in the digital realm. There are specific aspects of contestation that characterize human rights governance models in the internet realm. New human rights claims tend to clash with established frameworks. In the context of digital rights, the diversity of discursive frameworks and regulatory narratives is manifested through the coexistence of horizontal and vertical models of regulatory governance in the internet realm. The existing regulatory and ideological status quo is not aligned with the emerging new realities. Joanna Kulesza offers a multi-stakeholder approach to internet governance, as a distributed policy-making model based on voluntary cooperation among key actors typically identified as the state, the business sector, and civil society operating according to their respective roles through the principles of consensus and a working code.[226]

One of the impacts of technology on human rights, which has given rise to new human rights claims, refers to the development of neuro-rights. Neuro-rights emerged in response to the rapid development of neurotechnology, which has the potential to transform how humans understand and treat the human brain. However, these technologies also present significant ethical and social challenges related to the protection of individual rights, privacy, and mental autonomy.[227] The emergence of neuro-rights is inseparable from the inability of existing human rights to provide adequate protection against the threats and risks posed by these developments. The development of neurotechnology raises questions about how convincingly current human rights claims can provide adequate protection, and what risks or harms might arise from the introduction of these new human rights. New human rights claims face the challenge of how to legally ground these new human rights claims. Meanwhile, new human rights are defined as rights that, at the time of their inception, were not explicitly recognized in any human rights treaty, nor were they otherwise recognized as

[226] Ibid.

[227] Yan Cornejo, Neurorights, Neurotechnologies and Personal Data: Review of the Challenges of Mental Autonomy, *Journal of Digital Technologies and Law*, 2(3), 2024

rights in the legal sense.[228] The initiative to propose new human rights for the digital realm is a response to these new challenges to human rights in an increasingly digitalized world. Recent developments in efforts to strengthen the governance of artificial intelligence have contributed to this debate. However, is there really a need to recognize entirely new digital human rights, or is it sufficient to simply adapt or expand existing rights through interpretation to address new threats emerging from cyberspace? A new human rights initiative is a process that begins with the identification of new protection needs, followed by their formulation in the form of rights, and finally, the recognition and implementation of these protections.[229]

According to Yuval Shany, in some cases, the normative gap between offline human rights and the needs and interests of online users has reached a disturbing level. This situation suggests that adapting existing rights is no longer feasible or will produce highly inadequate outcomes. In such circumstances, developing new human rights, such as the right not to be subject to algorithmic decisions or the right to be forgotten, may be a worthwhile step.[230]

The limitations of international human rights law, according to Shany, place digital rights users in a state of uncertainty regarding the risk of receiving human rights protection:[231]

Navigating between old and new norms involves a complex legal policy dilemma. The creation of new norms within international human rights law does not necessarily necessitate the introduction of a new international human rights legal framework, but rather highlights the shortcomings of the existing framework. However, recognizing the inconsistency of rights applicable in the offline realm without a new set of human rights provisions in place to protect online users

[228] Nora Hertz, Neurorights – Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought, Neuroethics 16:5 (2023)
[229] Wolfgang Benedek, Is There a Need for New Digital Human Rights in AI Governance? Tiina Pajuste, (ed.), Human Rights in the Digital Domain: Core Questions, (Cambridge: Cambridge University Press & Assessment, 2026)
[230] Yuval Shany, Digital Rights and the Outer Limits of International Human Rights Law, German Law Journal 24, (2023),
[231] Ibid.

creates the risk of individuals being left in limbo, facing a protection gap. At the same time, clinging to existing international human rights legal norms, even when they are increasingly perceived as irrelevant, also results in a lack of protection for online needs and interests.

At the national level, comprehensive protection of fundamental human rights in the digital era is also limited because digital rights have not yet been enshrined as constitutional rights. According to Juliane Müller, addressing rights protection at the constitutional level offers a stronger and more lasting framework for addressing emerging digital threats than relying solely on conventional laws. As digital technology increasingly impacts the exercise of civil and political rights, as well as other fundamental freedoms, robust constitutional guarantees are essential to address new challenges ranging from unauthorized surveillance and censorship to algorithm-based governance and data monopolies.[232] Therefore, enshrining digital rights in the constitution offers a unique, robust, and lasting framework for protecting fundamental rights from the new challenges of the digital era. The protection of digital rights will be even stronger, given that constitutional provisions are more difficult to amend and hold a higher status than laws. The constitutionality of digital rights serves as a solid foundation for the protection of fundamental rights and freedoms in the context of ever-evolving technology. By embedding digital rights in the constitution, countries can ensure consistent protection. At the same time, this measure also provides a stronger oversight mechanism to prevent abuses of power by governments, such as unauthorized surveillance or censorship, as well as potential overreach by private actors, including large tech companies or entities with data monopolies. Constitutional recognition establishes clear standards for ethical and accountable corporate behavior and sends a strong signal, both domestically and internationally, that digital rights are taken seriously and protected at the highest legal level.[233]

[232] Juliane Müller, Rights in the Digital Age, https://www.idea.int/publications/catalogue/html/rights-digital-age , Accessed on 1 May 2026
[233] Ibid.

In this context, human rights are established and protected by law, whether through international treaties, national constitutions, or various laws. Efforts to ensure these laws are enforced, including by bringing certain cases to court, have not yet brought justice to victims. Courts are not always friendly platforms for upholding human rights. Costly delays, obstructive procedural rules, legal maneuvers that exploit existing legal loopholes, and judges' lack of empathy, whether individually or in combination, can lead to cases of injustice being dismissed. The risk of failure is even higher in countries where judicial independence and impartiality are in doubt. Judges may be reluctant to uphold human rights when repressive and/or discriminatory laws enjoy widespread support and are fully endorsed by politicians.[234]

At the same time, with the advancement of digital technology, digital media and social media now offer important new tools for social movements, activists, and critics of the state. At the same time, these tools also substantially expand state surveillance and repression against these actors. The use of digital surveillance by states has long been ongoing. This surveillance can take many forms and allows governments to gather intelligence that can be used to target specific individuals or groups. For example, dual-purpose technologies, such as deep packet inspection, allow operators to monitor internet traffic and content. Similarly, social media can be monitored in a similar way. While conventional surveillance is often conducted on specific targets or smaller target groups, digital repression allows surveillance to occur on a large scale when conducted with the involvement of Internet Service Providers.[235]

Ongoing practices demonstrate that covert surveillance can be conducted by a variety of private actors. First, individuals and groups can engage in online surveillance. Second, corporations also play a significant role in this area, either independently or through partnerships with governments. Governments and corporations can contract directly with hacking groups or collaborate with them

[234] Defending Human Rights in Court, https://www.openglobalrights.org/courts/ , Accessed on 1 May 2026
[235] Jennifer Earl, Thomas V. Maher, Jennifer Pan, The digital repression of social movements, protest, and activism: A synthetic review, Earl et al., Sci. Adv. 8, (2022)

indirectly through intermediaries. Furthermore, the phenomenon of surveillance capitalism has emerged, enabling corporations to simultaneously conduct large-scale and micro-scale surveillance targeting users' actions and interests. Furthermore, some existing policies benefit social media companies and governments seeking to suppress online activism. Companies have profited by selling users' personal data to law enforcement, selling the technology needed for network-based surveillance to governments, selling spyware that leverages zero-day exploits to turn mobile phones into mobile surveillance devices, and selling artificial intelligence devices used for mass surveillance that can easily be repurposed for repressive purposes. Companies such as NSO Group, Gamma Group, and Hacking Team provide states with access to exploitation, hacking, and surveillance services.[236]

The use of spyware is largely conducted in secret and with limited oversight, governments use spyware to target and collect information about civilians. This has led to numerous human rights violations against civilians, directly perpetrated by repressive states and enabled by spyware companies. Spyware targeting vulnerable civilians, such as journalists and human rights defenders, presents a complex challenge to accessing justice. Individuals may have different conceptions of what justice should look like in the context of redressing the harms they have suffered. Furthermore, individuals may face unique barriers depending on their context.[237] Targeted spyware attacks can give attackers real-time access to location and communication data and pose a real physical threat to the target. In this regard, spyware attacks are often accompanied by arbitrary detention, torture, and extrajudicial killings. The case of Loujain Al-Hathloul, a Saudi female human rights defender, illustrates this link. In legal proceedings in the United States, Al-Hathloul claims the use of spyware to spy on her communications and movements led to her arbitrary arrest by the United Arab Emirates and subsequent transfer to Saudi Arabia. Upon arriving in Saudi Arabia, Al-Hathloul was then detained, imprisoned and tortured.[238]

[236] Ibid.
[237] Siena Anstis & Jillian Sprenger , op.cit
[238] Ibid.

While the UN has affirmed its commitment to universal human rights online, just as it does in the real world, these principles only truly matter when violators face consequences, and the real world is any indicator. Numerous cases have shown personal data being used to undermine democracy, cyberattacks being launched to cripple critical infrastructure, or zero-day security flaws being exploited to infect devices with ransomware, yet the perpetrators almost never face justice.[239]

The development of data-driven technology has led to new injustices and become a source of increasing harm to individuals and communities. Meanwhile, accessing justice and redress in today's digital society is difficult and, in some cases, nearly impossible. There is a gap in accountability related to the rise in digital harm. Furthermore, policy responses to behaviors that result in such harm are inadequate. This situation creates a secondary problem: victims of digital harm lack a clear path to justice.[240] Harm caused by technology may occur online, but the harm it causes persists beyond digital and physical boundaries. What happens in the digital world spills over into the physical world, and what often appears to be a violation of privacy is actually a violation of self-determination and personhood. Protecting the right to self-determination and personhood requires recognizing that digital rights encompass all human rights and should not be limited to a limited set of civil and political rights, as the use of digital technology has a growing impact on all human rights. Algorithms used to predict and influence people's behavior impact freedom of thought. Other automated systems reinforce existing racial (ethnic) or social biases, thereby institutionalizing discrimination and other harms. Therefore, protecting digital rights must encompass all forms of self-determination and personality that are

[239] Marietje Schaake, Internet governance needs tough love, 2019, see, https://www.gwi-boell.de/en/2019/11/18/internet-governance-needs-tough-love , Accessed on 5 May 2026

[240] World Economic Forum Global Future Council on Data Policy, AI for Humanity and Media, Entertainment and Sport, Pathways to Digital Justice, White Paper, World Economic Forum, 2022

directed towards digital justice.[241]

In general, digital justice is understood in its corrective sense concerns redressing past wrongs, that is, harms that have been done to individuals or groups. Often, such corrective efforts are undertaken by imposing correlative responsibility on the perpetrators of the wrongdoing. However, corrective injustice can occur, for example, when the magnitude of the harm is underestimated or completely overlooked, when accountability is lacking, or when there are no effective avenues for redressing the harm to individuals or groups whose digital rights have been violated. However, given the critical knowledge gaps and the level of uncertainty surrounding the lack of accountability involved, it is important to recognize that even the best efforts to address these harms may be insufficient. One challenge relates to characterizing the potential new types of harm that data-driven technologies may cause. For example, artificial intelligence systems reduce individuals' gender identities to binaries, which has real consequences. When individuals and their communities are unrepresented, they lose the ability to effectively advocate for their human rights and fundamental freedoms.[242]

Another challenge arises from the fact that most moral and legal frameworks rely on the clear identification of a responsible wrongdoer who is obligated to restore the victim's dignity and reputation in some way or to provide restitution or compensation to the victim for the harm suffered. However, in many cases involving data-driven and predictive analytics, the allocation of such responsibility is complicated by online anonymity, the large number of actors involved in the process, and the so-called problem of many hands. Furthermore, even when there is a clear entity to which responsibility and blame can be assigned, establishing the facts and extent of harm can be challenging. The difficulty is most pronounced in cases of algorithmic opacity, namely, cases where the basis on which a predictive algorithm makes or recommends a decision remains incomprehensible to humans, including its users and

[241] Ibid.
[242] Ibid.

developers.[243] Furthermore, the lack of transparency presents challenges in identifying potential harm. This situation is compounded by the fact that many of the technical approaches used to make such algorithms interpretable are fragile and unreliable or insufficiently grounded in the specific purpose for which the interpretation is based. A further challenge, even when technical means to identify harm exist, is the practical barriers to obtaining redress that need to be considered. These barriers may include placing an undue burden on victims to provide evidence of harm. This becomes even more difficult for victims when the institution accused of causing harm is the gatekeeper to this evidence, thus reinforcing existing injustices and power imbalances.[244]

These challenges generally relate to access to justice, which refers to the right to obtain justice. This can include access to the formal justice system and guarantees of due process, the right to a fair trial, and the enforcement of judgments. The Guiding Principles on Business and Human Rights emphasize that access to justice in international human rights law also requires access to remedies, which may include apologies, restitution, compensation, punitive sanctions, or the implementation of mechanisms to prevent future harm. Justice and its remedies can be pursued at the domestic or international level and can involve formal or alternative dispute resolution and law enforcement mechanisms. Access to justice, of course, involves the social context in which the justice system operates. Often, social or other barriers face individuals in accessing redress mechanisms.[245]

To date, the primary avenues for access to justice initiated by civil society have included civil litigation and advocacy for domestic legislative reform and other government action to control the spyware industry.[246] This litigation will confront various attempts by spyware vendors to obstruct the path to accountability, such as identity changes, opaque corporate structures, and movement between jurisdictions. Individual victims of spyware, particularly when

[243] Ibid.
[244] Ibid.
[245] Siena Anstis & Jillian Sprenger , op.cit
[246] Ibid.

targeted by powerful and well-resourced states, face high costs in pursuing legal action against spyware vendors and procedural challenges in demonstrating causation and culpability. In addition to the costs of litigation, individuals may suffer physical, financial, or other retaliation against themselves or their affiliates, including family, friends, colleagues, and healthcare providers.[247] In this context, according to Sara Ann Brackett and Jen Roberts, challenges to pursuing litigation-based accountability for spyware use include:[248]

1) Awareness of individuals targeted by spyware is still lacking

Individual awareness of being targeted by spyware is a crucial prerequisite for accountability. Spyware is designed to remain undetected by victims and can often only be detected through advanced forensic analysis. Without knowledge or suspicion of spyware use, individuals whose devices are hacked may be unable to seek justice or take precautions to protect themselves, their contacts, or their communications. Awareness of the impact and dangers of spyware has increased in recent years due to the significant investigative work of civil society. In high-profile cases such as attacks on human rights activists, journalists, and lawyers in Mexico, victims and their affected family members have collaborated with research and advocacy groups, including Citizen Lab, Amnesty International, and Access Now, to link suspicious text messages to attempts to install NSO Group's Pegasus on their devices. In recent cases, including the use of Paragon's Graphite malware against European journalists and NSO Group's Candiru malware against prominent civil society members in Catalonia, threat alerts from Apple and WhatsApp have prompted forensic investigations by Citizen Lab, which confirmed the presence of spyware. Without suspicion and subsequent confirmation of spyware use, individuals cannot take legal action against spyware vendors;

2) Lack of clarity about spyware vendors

[247] Sara Ann Brackett and Jen Roberts, 404 Accountability not found: Spyware accountability through software liability, Atlantic Council, 2025
[248] Ibid.

Another obstacle to spyware vendor accountability is the opacity of the spyware market. The Atlantic Council's *Mythical Beasts* report, which mapped the spyware ecosystem, outlined the tactics used by spyware vendors to obscure their identities. Spyware vendors frequently change their names, in some cases multiple times, to conceal their identities and potentially mitigate the business impact of negative reporting. For example, vendor Candiru Ltd. changed its name four consecutive times from 2016 to 2020 and now operates as Saito Tech Ltd. Numerous entities in the spyware market have changed names. Without consistent naming conventions and legal records, civil society organizations, targeted individuals, and companies are often unable to identify the responsible entities and individuals, allowing spyware vendors to operate with impunity. Spyware vendors also engage in corporate restructuring, including opening branches, developing subsidiaries, creating strategic partnerships, or establishing supplier relationships, which can make it difficult to attribute spyware incidents to specific entities. Without attribution of spyware infections to specific vendors, litigation cannot result in accountability for specific harms suffered by specific vendors.

3) Difficulty in establishing jurisdiction

Lawsuits against spyware vendors also face the challenge of determining the proper venue for trial. In lawsuits against spyware vendors, the relevant physical location can vary and become difficult to determine. Determining jurisdiction is a significant challenge because it involves verifying the nationality of the company or country where the spyware vendor operates, the location of the targeted devices, the nationality and residence of the targeted individuals, the location of the companies and computing infrastructure that provide the targeted technology products, and the legal status of the purchasers of the spyware software. The dispersed and decentralized nature of the losses in these cases can make it difficult to determine which court is the appropriate avenue for claims against the spyware vendor and, therefore, which court has jurisdiction to hear a case.

4) Risk of disclosure of technical information

Another barrier to successful litigation against spyware vendors relates to the risk of revealing detection methods and research sources to the vendors. Efforts to identify spyware based on technical footprints or behavioral patterns of spyware vendors allow for attribution of spyware infections to specific vendors or spyware devices. However, publicly disclosing such information can risk tipping off spyware vendors to details researchers rely on to detect infections and spyware infrastructure, enabling the adoption of new tactics. This disclosure allows vendors to stay ahead of targeted individuals. In September 2024, Apple dropped its ongoing lawsuit against NSO Group, citing a preference for avoiding the risk of revealing threat intelligence and detection capabilities during litigation. This illustrates the tradeoff between the benefits of publicly disclosing indicators and the risks of informing spyware vendors about detected techniques. Researchers and technology companies may choose to disclose details to inform and protect the public, exposing information such as domain names, email addresses, and process names used by spyware vendors. This disclosure often prompts spyware vendors to adopt new infrastructure configurations to evade detection and attribution. Keeping certain technical indicators of spyware infections secret can also allow for attribution of future attacks, as demonstrated by the Citizen Lab report on FORCEDENTRY. Furthermore, spyware vendors have demonstrated that their infrastructure can recover from public exposure and continue operating, as was the case with the Intellexa Consortium. In at least three cases beginning in 2023, Intellexa Consortium's infrastructure was unmasked by civil society researchers from Amnesty International, Recorded Future's Insikt Group, and Sekoia. The civil society research resulted in the internal shutdown of Intellexa Consortium's infrastructure, impacting the consortium's ability to spread or maintain infections. This infrastructure shutdown was further exacerbated by US Treasury sanctions against Intellexa Consortium members in 2024.

Human rights violations resulting from the proliferation of the spyware industry continue to occur. This stems from a lack of political will to take the

necessary steps to control the spyware industry and protect human rights. Arguments used to justify the use of spyware for law enforcement and national security purposes. Many countries, including liberal democracies, continue to use spyware or similar technologies or allow the industry to flourish within their borders. Overall, without government recognition that the harm caused by digital spyware outweighs its financial and political benefits, there will likely be a persistent lack of political will to make meaningful changes.[249] Therefore, efforts to achieve spyware accountability through legislative safeguards remain significant. These legislative measures, if implemented, could reshape incentives for technology companies to assist in the pursuit of spyware accountability. Thus, legislative measures provide a modality for demanding accountability for spyware use. The next step, litigation and other accountability actions undertaken by technology companies such as Apple (iMessage, iPhone), Google (Android), and Meta (WhatsApp), while likely to face obstacles, these companies possess unique capabilities to counter the risks and dangers of spyware and overcome these obstacles. Litigation and preventative action by technology companies do not always involve direct compensation to victims or justice for previous harms, but can act as important preventative measures to prevent future spyware harms, complementing other approaches to holding spyware users accountable.[250]

The success of corporate lawsuits filed through litigation mechanisms in the United States demonstrates the urgency of involving corporations in demanding accountability for the use of spyware. Corporate plaintiffs who allege to be victims of NSO Group have been more successful in overcoming procedural obstacles than individual plaintiffs. Two corporate lawsuits, one filed by Apple and the other by WhatsApp, successfully overcame NSO Group's jurisdictional challenges. NSO Group ultimately held itself accountable in the WhatsApp case, largely due to its refusal to provide information to opposing counsel during the evidence-gathering process. Ultimately, on 6 May 2025, a jury awarded

[249] Siena Anstis & Jillian Sprenger , op.cit
[250] Sara Ann Brackett and Jen Roberts, op.cit

WhatsApp $167 million in damages. NSO Group has asked the court to drastically reduce the amount or order a retrial.[251] However, in September 2024, Apple decided to withdraw its lawsuit, in part because it would have been forced to disclose information about Apple's security practices that predatory spyware companies had sought for years. According to Apple, the withdrawal was based on user protection concerns:[252]

Apple currently uses threat-intelligence information to protect every user worldwide, any disclosure, even under the strictest controls, would compromise this information.

On the other hand, individual lawsuits have failed due to procedural hurdles. At least three lawsuits have been filed in U.S. federal courts against NSO Group on behalf of individual victims alleging violations of various federal and state laws following attacks with the Pegasus spyware. Procedural challenges in court have slowed or even prevented these cases from reaching the brink of litigation, leaving victims in limbo with no recourse. These plaintiffs face significant jurisdictional hurdles, sometimes having their cases dismissed on these preliminary grounds after months of court battles. Judges have rejected attempts to hold NSO Group accountable for violating state and federal laws prohibiting hacking and unauthorized data collection, arguing that the company lacks sufficient ties to the United States or specific states.[253]

Judges have also dismissed cases on the grounds that the United States is not the proper forum for these cases, and that the lawsuits should be filed in jurisdictions other than the United States. For example, the Fourth Circuit Court recently upheld a federal district court in Virginia that dismissed a lawsuit filed by the widow of murdered journalist Jamal Khashoggi against NSO Group for lack of personal jurisdiction. This procedural challenge prevented the judges from addressing the merits of the case against NSO Group, leaving victims of the

[251] Nadine Farid Johnson, Unlocking Justice: A Policy Roadmap for Victims of Spyware, 2025, https://knightcolumbia.org/blog/unlocking-justice-a-policy-roadmap-for-victims-of-spyware , Accessed on 6 May 2026
[252] Ibid.
[253] Ibid.

spyware invasion in limbo and without recourse in U.S. courts, even though they suffered violations of privacy, security, and freedom of expression caused by the company's technology.[254]

The use of *forum non conveniens* is of particular concern in human rights cases where U.S. courts may be the only reasonable venue for such cases. While U.S. district courts may be inclined to direct parties in spyware cases to litigate in the country where the defendant is established or where the alleged attack occurred, the reality is that bringing such cases to court in those jurisdictions is unlikely. For example, NSO Group is founded in Israel, while the Israeli government took extraordinary measures to undermine the WhatsApp litigation, as The Guardian reported. And courts in countries like Saudi Arabia, the United Arab Emirates, or El Salvador, where targeting human rights dissidents and journalists is commonplace, are not appropriate venues for justice. As the plethora of emerging spyware litigation demonstrates, potential plaintiffs face procedural challenges in bringing cases in U.S. courts or elsewhere around the world, threatening a situation where no court will be willing to hear these victims' cases on the merits.[255]

A pathway to redress through litigation is crucial for spyware victims. Options for potential plaintiffs are inconsistent and unclear, yet the harm and security threats associated with spyware continue and grow relentlessly. Policymakers must address this fundamental imbalance and create a level playing field for spyware victims, enabling a pathway to redress.[256]

I. The Urgency of Developing a Human Rights-Based Accountability Ecosystem for Spyware Use in Indonesia

I.1. Legal Void Regarding the Use of Commercial Spyware and the Procurement of Commercial Spyware

An Amnesty International report shows that even extensive human rights

[254] Ibid.
[255] Ibid.
[256] Ibid.

protections will not protect civilians from highly invasive spyware.[257] In Indonesia, although the International Covenant on Civil and Political Rights (ICCPR) has been ratified through Law No. 12 of 2005, the substance of the Covenant has not been fully translated into operational domestic law. Ratification of the ICCPR represents Indonesia's initial commitment to recognizing a catalog of fundamental rights for citizens, such as the rights to freedom of expression, assembly, personal security, and protection from arbitrary detention. Unfortunately, this commitment has not yet been translated into specific regulations governing the legitimate use of spyware and surveillance. To date, Indonesia still lacks specific regulations that explicitly and comprehensively define the use and procurement of spyware as separate normative objects. This legal vacuum could perpetuate unaccountable surveillance practices that threaten fundamental rights, undermine democratic stability, and endanger national security.

This regulatory vacuum at the national level is inextricably linked to the complexity of formulating policies related to surveillance technology at the global level. Regulation is complicated because spyware is a subset of offensive cyber capabilities that lacks a concrete form, making its technical nature difficult to understand. This difficulty is compounded by the lack of a clear framework for defining the scale of operations and accurately measuring the impact of these tools. The impact of this technology on the international balance of power remains a matter of debate. When states and non-state actors gain access to and utilize offensive cyber capabilities, instability in cyberspace increases. This issue becomes increasingly pressing as the number of state-sponsored cyber actors increases and the severity of cyberattacks increases. Therefore, policy development should not be bogged down in futile attempts to completely block spyware proliferation, but rather should focus on strategies to reduce the technology's utility and influence the incentive structure of the actors involved in its deployment.[258]

---

[257] Amnesty International, *The Predator Files: Caught in the Net,* Index: ACT 10/7245/2023, 9 October 2023, https://www.amnesty.org/en/documents/act10/7245/2023/en/ . Accessed on August 2025.

[258] Cardillo, Fischer, and Kekre, *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*.

However, efforts to influence these incentive structures often clash with the reality of the commercial spyware market, which remains under-regulated. While controlling market transactions is crucial, commercial trade is not the sole source of security threats, given that many similar capabilities are developed internally by state institutions. To date, international policy remains mired in debate over the parameters of legitimate spyware use. This lack of clarity in standards makes commercial sales volume an unsuitable indicator of responsible technology use. A transaction may be procedurally legitimate, yet still lead to destructive misuse. History shows that the commercial market is only one part of a broader proliferation challenge. In fact, systematic human rights violations often occur through the use of spyware vertically against one's own citizens, as well as diagonally against foreign nationals and diaspora groups under the pretext of state security interests.[259]

This ambiguity often stems from inconsistent terminology, which has been a major obstacle to policy formulation. Jean Robert et al. emphasize that the effectiveness of regulation depends heavily on a precise definition of spyware that clearly distinguishes it from other surveillance technologies. Within this framework, spyware is defined as a technology or tool that operates entirely without the consent or knowledge of the target, or any other individual with authorized access to the target device (such as a mobile phone or computer). This definition excludes:[260]

1. Technology without access to the target device: This includes software that does not enter the target device's system at all. This tool only works externally, namely collecting data moving on the communication line (such as data packet tapping or sniffing via cable/Wi-Fi).
2. Tools with physical access: Includes products that require direct physical contact with the target device (such as stalkerware) or must

[259] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."
[260] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

be in close proximity to the device (such as forensic tools and mobile tapping).

This restriction is done intentionally to prevent mixing various other surveillance instruments into the spyware category.[261]

Based on this definition, 435 entities were identified as operating in the spyware market between 1992 and 2023. This identification includes vendors and their subsidiaries, senior officials, and investors. This mapping aims to create transparency in the often obscured supply chain, allowing policymakers to track the flow of capital and technology that facilitates human rights violations. The following table details the key actors:[262]

Supply Chain Elements	Description/Role
Spyware vendor	A commercial entity that develops, support, and sells spyware to end users. This development and support may include vulnerability research and exploit development, malware payload development, technical command and control, operational management, and training and support, but not necessarily all of them.
Individual	A person directly involved with a vendor or supplier, or an entity directly related to a vendor or supplier. This individual may be a company founder, senior management officer, or investor.

[261] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."
[262] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

Supplier	Suppliers sell components or services used to develop spyware products but do not directly develop or operate the spyware or similar services. Suppliers may sell vulnerability or exploit subscription services to vendors who then develop the actual software. Suppliers are a crucial but often overlooked part of this market.
Partner	A company connected to a spyware vendor, although the nature of the relationship can take several different forms. First, the partner may be unrelated to the development of the spyware itself but essential to other operations of the vendor (e.g., marketing or sales services). Second, the partner may provide complementary surveillance products, such as telecommunications eavesdropping devices or ways to process data collected from the spyware, such as location data mapping tools.
Holding company	A type of business entity that owns outstanding shares of other companies. Its primary purpose is to control and manage one or more of its owned companies, rather than producing its own goods or services. A holding company can own a variety of assets, including shares of other companies, real estate, patents, trademarks, and more. By holding control over other companies, the holding company can influence or direct their management policies and decisions. This structure can provide benefits such as risk management, tax advantages, and simplified control over multiple businesses.
Subsidiary	A company in which more than fifty percent of its shares are owned by a parent company or holding company. A subsidiary is separate and legally distinct from its parent or holding company, typically reflected in its independence in governance, finances, taxes, and liabilities. However, the parent company often has significant influence over its subsidiaries.

Based on the operational spyware market there are six different tendencies, namely:

1) The majority of identified entities are domiciled in Israel, India, and Italy;
2) There are a lot of serial/moving entrepreneurs;
3) Strong partnerships between spyware and surveillance hardware vendors;
4) Deliberate and repeated efforts by companies to change their identity and even their corporate structure;
5) The movement of corporate structures across strategic jurisdictional boundaries;
6) Significant cross-border mobility of capital supports the development and sale of spyware.

These six trends need to be emphasized in developing policies governing accountability for spyware use. The focus of the policy should not only target legal entities but also consider the following industry dynamics:[263]

1) Serial/moving entrepreneur

There is a recurring pattern of employees, including founders, leaving their initial companies to found and work for others. This is not unlike other startup cultures where this type of serial entrepreneurship is common. However, in this market context, the risks are significantly greater given the fundamental similarities in the technical functionality of spyware products and the strong personal relationships between customers (government agencies) and founders and senior employees. The analyzed data sets show that vendor and supplier

[263] Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

founders often remain involved in the industry by moving from one entity to another.[264]

Therefore, oversight should no longer be limited to corporate entities but should instead target the mobility of individual talent moving between companies. To curb talent movement between vendors, export licensing bodies could request more detailed information about key personnel and their prior employment to help identify individuals categorized as repeat violators of other jurisdictions' laws and policies. Policymakers should also consider focusing on individuals when attempting to curb malicious activity by vendors, rather than solely on vendors as business entities, given the fluidity of talent across companies.

2) Partnership with Hardware Surveillance

Spyware vendors sometimes partner with hardware-based surveillance companies whose products may complement the functionality of their spyware. Nine vendors or suppliers have at least one official partner, five of which have specific alliances with hardware companies.[265]

While collaboration between complementary products is commonplace in

[264] NSO Group, arguably the most notorious spyware vendor, is a prime example of this phenomenon. Founded in 2010 in Israel, the company is the developer of the Pegasus spyware. Despite EU investigations and US regulatory action, the company continues to operate branches in the United States and Luxembourg, along with subsidiaries in Bulgaria and Cyprus. Another example is vendor Quadream Inc., known for its Reign spyware, founded in 2016 in Israel by former NSO Group employees and former military officials and known as Kvader Ltd. in Israel. Like Quadream Inc., Interionet Systems Ltd. (Interionet) is an Israeli vendor founded in 2015 by former NSO Group employees. An Israeli businessman, a shareholder and board member of NSO, also sits on Interionet's board. See Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[265] The most active example of this partnership is the Intellexa Consortium, which encompasses relationships between seven different hardware companies. Formed around the founders in 2018, the Intellexa Group consists of several companies, including Cytrox AD, WS WiSpear Systems Limited (also founded by the same founders), and Senpai Technologies Ltd. In 2020, the Intellexa Group expanded to include Intellexa SA, formerly known as Intellexa Single Member. Cytrox AD was formed in 2017 in North Macedonia and developed the spyware known as Predator. WS WiSpear Systems Limited specializes in intercepting targeted Wi-Fi signals and remotely extracting passwords and communications, and Senpai Technologies Ltd. is an open-source intelligence company specializing in analyzing data from spyware-infected phones. See, Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

business, synergies within the spyware market warrant special attention. This phenomenon underscores the need for policies to target the entire market ecosystem through cross-border collaboration, as regulations focused solely on a single vendor or jurisdiction will be limited in effectiveness. To strengthen oversight, regulations regarding the types of support provided to vendors serving government agencies need to be tightened. This includes expanding transparency through Know Your Vendor principle to encompass the entire partnership chain beyond the initial transaction. This recommendation is particularly urgent given the constantly evolving nature of vendor identities and the complex relationships between the spyware market and the rest of the electronic surveillance industry.

3) Vendor identity changes

Spyware vendors frequently change their official names and even overhaul their entire corporate structures. This strategy is not without reason; these identity changes are deliberately carried out to disguise their operational footprint and minimize the impact of negative press or scandals. Although a company's official name frequently changes, public reports typically continue to refer to the entity by its most popular name. This creates a dangerous loophole because it can obscure the vendor's ongoing operations and hinder the due diligence efforts of researchers, policymakers, and investors. Data shows that the average entity in this market changes its name more than once, with each name lasting an average of only 4.5 years. This "chameleon" phenomenon complicates long-term track records and allows problematic vendors to continue securing funding or new contracts under seemingly clean identities.[266]

[266] To put the shifts in perspective, Holding companies had the highest percentage of name changes at 34.4 percent, followed by Vendors (14.3 percent), Partners (20.8 percent), Suppliers (five percent), and Investors (2.1 percent). The most frequently changing identity was the company originally known as Candiru Ltd, which changed its name four times over a nine-year period, and at the time of this writing is known as Saito Tech Ltd. The vendor originally known as Candiru Ltd was founded in 2014 in Israel. Candiru Ltd has sold products to Hungary, Spain, and the United Arab Emirates, all of which used spyware for political repression against the opposition and civil society. The group's annual name changes between 2016 and 2020 were not accompanied by changes in corporate structure. In 2021, Candiru Ltd and its related names were added to the United States Entity List along with NSO Group. While in common discourse, the vendor is often referred to as Candiru Ltd,

Various examples illustrate why tracking vendors is difficult for policymakers and researchers. Shifting vendor identities creates the illusion that a vendor has ceased operations when, in fact, they operate under a different name. This image is further complicated by subsidiaries and branches, as they can also quickly change names. This complexity is further compounded by networks of subsidiaries and branches, which also frequently change names within a short period of time. To counter these disguise tactics, policy solutions must focus on tracing the relationships between the individuals and investors behind these entities. A concrete step could be to tighten spyware procurement procedures through mandatory Know Your Vendor principle, which require disclosure of supplier relationships down to the first and second tier. Furthermore, increased transparency and consistency in company registration are essential to map the interconnectedness of these identities, even when operating across multiple jurisdictions.

4) Strategic Jurisdictional Shift

Some vendors are establishing networks of subsidiaries, branch offices, and even partnerships that cross strategic jurisdictional boundaries. This relocation can offer a variety of location-specific benefits, from facilitating sales into the EU market with EU-domiciled companies to establishing branches in countries with more lenient laws.[267]

National legal structures based on sovereign boundaries often fail to address spyware vendors who deliberately establish cross-border subsidiary networks to evade export controls. This jurisdictional arbitrage creates significant operational and supply chain opacity, particularly when vendors relocate to less

this report refers to all vendors by their current legal name, which for Candiru Ltd is Saito Tech Ltd. See, Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

[267] In 2017, Israeli vendor Quadream Inc. established a supplier, InReach Technologies Limited, in Cyprus. According to Quadream Inc., in court filings, the sole purpose of promoting Quadream Inc.'s products in the European Union. InReach Technologies Limited's financial structure also includes AIL Nominal Services Ltd. (AIL), also established in Cyprus in 2010 as a holding company, with an individual with ties to the Ministry of Defense. See Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

regulated jurisdictions to blunt the effectiveness of international policies. This complexity is further exacerbated by highly dynamic cross-border capital flows, making holding companies accountable increasingly difficult without measures that explicitly limit these loopholes.

5) Global Capital Mobility

Investors in spyware vendors frequently cross borders with their capital. Like other conventional markets, spyware vendors and suppliers have an investor base domiciled in various jurisdictions. Four jurisdictions most frequently represent investor origins: Italy, Israel, the United States, and the United Kingdom, accounting for 46.3 percent of all investors. The nature of spyware investments varies from venture capital, private equity, and government loans to outright acquisitions and direct equity ownership. Statistically, each vendor and supplier in this dataset has an average of 4.75 percent of identified investors. This suggests that their operations are supported by a fairly extensive funding network. For example, 14 US-based entities were identified as investing in this market, of which 12 invested in vendors based in Israel.[268]

The dynamics of cross-border capital flows demand close international cooperation, with the United States and the European Union playing a central role in implementing strict oversight of investor relations in the spyware market. Strengthening transparency, such as mandating beneficial ownership reporting, is crucial to support due diligence and deeper transaction reviews. For vendors outside the US, the proposed expansion of security reviews to outbound investments provides a legal basis for cataloging, or even blocking, capital flows to risky entities. Furthermore, the use of targeted sanctions, both against vendors and investors, is a crucial tool for limiting market mobility. While the use of

[268] A specific example of this trend is Paragon Solutions. Paragon was founded in 2019 in Israel. Several years later, in 2022, the company established Paragon Solutions US, a US-based subsidiary. Since its founding, Paragon has made a deliberate effort to penetrate the US market. Paragon Solutions also has two US-based investors. Battery Ventures, considered one of the world's leading venture capital firms and headquartered in Boston, is an investor in Paragon Solutions at the time of this writing. The company is also backed by Bloomberg Capital, another major US venture capital firm. See Roberts et al., "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights."

unilateral sanctions remains a hotly debated topic, this instrument remains a strategic option within the national security policy landscape to curb the proliferation of malicious surveillance technology.

Based on the results of the identification of the scope of the problem, Roberts et al. propose policy recommendations aimed at promoting greater transparency across the market, limiting jurisdictional arbitrage, and more effectively overseeing supplier and investor relationships. Furthermore, these policy objectives would address significant opportunities to limit the risks and losses arising from spyware proliferation. Recommendations that could be considered in developing a spyware use policy also include vendor behavior dimensions, a robust investor due diligence regime, information-rich government risk assessments prior to procurement, and credible legal support for greater long-term transparency in the market. Based on the scope of these recommendations, the accountability arrangements for spyware use are generally focused on several dimensions:

1) Mandate "Know Your Vendor" requirements

A key characteristic of spyware acquisitions should theoretically be due diligence, so a gap in current policy is the ability to conduct due diligence regarding vendor identities and changing supply chains. In this context, it is crucial to implement Know Your Vendor requirements that require spyware vendors to disclose supplier and investor relationships. This is a credible step toward better information about the spyware market segments that governments may be engaging with. Know Your Vendor would create a more consistent reporting environment on the spyware market, providing the ability to examine where their prospective supply chains might include companies on the restricted entity list before awarding contracts. Know Your Vendor would also enable long-term efforts to reduce government funding flowing to high-risk suppliers or vendors. A more effective version of these requirements could require disclosure of companies further up the supply chain, including suppliers to vendors' suppliers.

2) Improving registration of government-managed companies

Similar to Know Your Vendor, government-managed company registries are a resource for due diligence and accountability. They will play a crucial role in a more robust policy regime addressing cross-border movements or investments in spyware vendors. They will also be a crucial source of information for due diligence by potential investors and provide greater visibility into business entities operating in their respective jurisdictions. Therefore, for company registries to be a source of truth regarding a vendor's business and financial structure and history, they must be comprehensive, publicly accessible, and contain verified information. Some key points relevant to enhancing these registries are:

a. Expand the minimum scope of data recorded in registration

National regulations should specify requirements regarding the categories and related details included in company registrations. These requirements should include basic company information, such as: (1) name, registration number, payment ID, address, contact details, and registration date; (2) ownership details, including senior executives, management board, and beneficial owners; (3) number of employees, financial information, including balance sheets, cash flows, profit and loss statements, and investors; (4) name change history, and legal status of activities, such as liquidation, active, or bankruptcy. This information serves as a minimum requirement, but can be expanded to include merger and acquisition history, legal actions against the company, and active export licenses.

b. Expansion of Beneficial Ownership Identification

Better recognition of the beneficial owners of spyware vendors and suppliers would provide a powerful deterrent to many of the behavioral tendencies of commercial spyware companies. Further improvements to the identification of beneficial ownership would require companies to report individuals who own 25% or more of the company's shares and voting rights or exercise significant control over its management. Transparency of beneficial ownership is supported and monitored by several international organizations, such as the Financial Action

Task Force (FATF) and the OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes.

c. Publication of government-managed company registration data

Improved registries should provide public access to commercial spyware company data across all jurisdictions. Poor record quality hinders due diligence efforts by many parties. For example, a high-quality, publicly accessible company database would provide valuable information for a much better investor due diligence regime in the spyware market. It would also help level the playing field between regulators in different jurisdictions. It would enable cross-border collaboration in regulating the behavior of spyware vendors, suppliers, and investors. Furthermore, it would enable entities subject to customer due diligence, such as banks, notaries, and corporate service providers, to improve their verification processes and report non-compliance.

3) Enrich, audit and publish export permits

Export licensing requirements are a mechanism for governments to restrict the sale and use of certain products and services outside their borders. Export licensing is a complex area characterized by significant cross-country variability in standards, covered goods, and the application of broader public interest tests, such as human rights considerations. Authorities may even deprioritize human rights risks by citing opposing considerations, such as industry growth or perceived geopolitical influence that favor licensing approvals. Therefore, the application of export controls to spyware technology must maintain a balance between these diverse interests.

Some spyware vendors, such as the NSO Group, openly use the fact that their exports are licensed by government agencies as an indication of their legality. The UN Special Rapporteur on Freedom of Opinion and Expression has stated that the global export control framework and its national implementation in the regions where the NSO Group operates are inadequate to regulate surveillance technology or account for human rights impacts. Consequently, even if the NSO Group's exports are licensed, their exports and those of other

vendors could still pose serious human rights risks, particularly in jurisdictions where the legal framework governing the use of their products is minimal or non-existent. Strengthening the export licensing regime can be achieved in three ways. First, export control licenses for spyware and closely related services should include the names of all employees whose work has a material impact on the development of the product subject to the export license. Second, to ensure effective export controls domestically, governments should implement mandatory and regular audits of licensing practices and impose sanctions for violations. Third, audit reports and original export licenses should also be made publicly available through national licensing authorities.

4) Limiting Jurisdictional Arbitration by Vendor

Implementing policies outside a country's jurisdiction presents challenges and opportunities for spyware vendors and others seeking to circumvent policy controls. This extraterritoriality is often exploited by spyware vendors to engage in jurisdictional arbitrage and take advantage of intergovernmental inconsistencies. The Recommendation proposes limiting arbitrage measures by focusing on increasing barriers for vendors related to export licensing for electronic surveillance technology, including spyware, to leave one jurisdiction and requiring reporting of new branches and subsidiaries. Jurisdictional arbitrage by spyware vendors undermines the rule of law, the efficiency of policy oversight, and market integrity, and can fuel policy competition between different jurisdictions, with countries adopting lower-standard policy requirements to attract business and investment.

Therefore, policy development should focus on several key strategies. *First*, it should make it more difficult and expensive for vendors holding export licenses to exit a jurisdiction. This should include requiring public disclosure of any opening or closing of subsidiaries or branches by vendors licensed to export spyware.

Second, policymakers with existing authority to regulate inward investment should automatically review transactions that impact the ownership structure of domestic spyware vendors in any way. Vendors that fail to flag such transactions,

including if the information is disclosed through Know Your Vendor disclosure mechanisms, should be prohibited from participating in government procurement and/or have their export licenses suspended for a specified period. In the context of the spyware market, notification requirements would increase market transparency and help put regulators in different jurisdictions on a more level playing field. They would also allow key stakeholders, including civil society organizations, to have visibility into spyware vendors' operations and their compliance with regulatory requirements. Third, harmonization of these disclosure requirements should be part of collaborative mechanisms and intergovernmental cooperation. Effective barriers to the exit of these spyware vendors from the market would help increase the potential for domestic policy influence.

5) Provides greater protection against Strategic Lawsuits Against Public Participation (SLAPP)

One of the broader trends in demanding accountability for spyware use is the importance of open reporting through journalism and research. A recent, worrying trend threatens to undermine this reporting, as a number of spyware vendors are resorting to Strategic Lawsuits Against Public Parties (SLAPPs). At this point, it becomes strategic for states to choose the jurisdictions/hosting parties for the lawsuits. for victims of SLAP lawsuits to raise this issue through diplomatic channels to protect victims and demand accountability for the use of commercial spyware.

In addition to the aforementioned dimensions, in relation to policy development, it is necessary to learn from the German experience, where cybersecurity strengthening is carried out through a comprehensive legal framework that goes beyond simply addressing cyberespionage. German legal regulations also cover digital crimes such as unauthorized access to electronic systems, data theft, and the production and distribution of intrusion tools.[269] These

[269] Mohamad Djafar Sodiq et al., "Cyber Espionage Policy and Regulation in Indonesia," *IDEAS: Journal of Education, Social, and Culture* 10, no. 4 (November 2024), https://jurnal.ideaspublishing.co.id/index.php/ideas/article/view/1909/799 .

regulations are outlined in the German Criminal Code (*Strafgesetzbuch*). More specifically, German cybersecurity regulations are designed to protect sectors categorized as critical infrastructure, including energy, water, telecommunications, transportation, and healthcare. Operators in these sectors are required to implement adequate cybersecurity standards and measures to protect their systems from various cyberthreats, including digital espionage and sabotage. Within this institutional framework, the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) serves as the central authority for managing national cybersecurity. The BSI is responsible for promoting the implementation of cybersecurity practices, providing technical guidance to public and private entities, and coordinating responses to cyber incidents. Germany's robust and clear legal framework serves as a bulwark against cyber threats. This, coupled with a transparent legal framework, ensures clarity and efficiency in addressing cyber threats.[270]

In the Indonesian context, the use of spyware is indirectly regulated through various laws and regulations related to cybersecurity, personal data protection, wiretapping, and cybercrime. The lack of specific regulations for the procurement of sensitive technology has the potential to create ambiguity in procedures and oversight. This is also susceptible to abuse, particularly due to the paradoxical nature of spyware devices: they can be used for national security purposes but also have the potential to violate privacy and freedom of expression. A summary of laws and regulations related to spyware in Indonesia is presented below.[271]

Legislation	Information
Law No. 19 of 2016 amending Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law);	Article 31: Prohibits unauthorized tapping of electronic information and Article 32: Prohibits unauthorized changes, deletions or tapping of electronic data.

[270] See Appendix 2
[271] Data source processed by FITRA

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) which regulates the protection of personal data in Indonesia, including data collected illegally through spyware.	Article 16: Data controllers are obliged to prevent unauthorized access to personal data and Articles 65 to 66: Regulate administrative and criminal sanctions for perpetrators who collect, use, or distribute personal data illegally.
Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation regulates electronic system security, including protection against threats such as malware and spyware.	Electronic system organizers are required to implement cybersecurity standards to prevent data misuse.
Law No. 35 of 2009 concerning Narcotics (Narcotics Law).	Regulates the expansion of wiretapping investigative techniques. In Article 78 paragraph (1) In urgent circumstances and investigators must conduct wiretapping, wiretapping may be carried out without prior written permission from the head of the district court. And paragraph (2) Within a maximum of 1 x 24 (one times twenty-four) hours, investigators must request written permission from the head of the district court regarding wiretapping as referred to in paragraph (1).

Cybersecurity mechanisms in Indonesia are built through a legal and institutional framework that places digital security as part of the national interest. The National Cyber and Crypto Agency (BSSN) serves as the primary authority in

formulating technical policies, securing government electronic systems, and coordinating the detection and response of cyber incidents across sectors. The cybersecurity regulatory framework is based on the ITE Law, the Personal Data Protection Law, and various regulations related to the implementation of electronic systems. These laws and regulations require electronic system administrators to protect data and systems from unauthorized access, leaks, and misuse, while also providing the legal basis for the state to prevent and address cyber threats. Indonesia also establishes special protections for vital information infrastructure and national vital objects, such as the energy, financial, telecommunications, and digital public services sectors. However, challenges remain in the form of fragmented authority and the need for stronger oversight to ensure cybersecurity policies remain aligned with human rights principles and personal data protection.

Up to the present, the authority to conduct wiretapping has been vested in various sectoral or separate regulations, such as the Electronic Information and Transactions Law (ITE Law), the Telecommunications Law, the Corruption Eradication Commission (KPK) Law, and others. The absence of a specific law providing a legal framework for wiretapping has resulted in inconsistent procedures and standards, potentially leading to abuse for purposes beyond law enforcement.[272]

The existence of a legal umbrella regarding wiretapping is important to provide procedural certainty, determine the authority of authorized institutions, and establish rules regarding permission from independent authorities such as courts, while also distinguishing between wiretapping for law enforcement (pro justitia) at the request of the Police or the Prosecutor's Office and wiretapping for intelligence or state security purposes such as the State Intelligence Agency (BIN) and the National Narcotics Agency (BNN). What is also important is how to ensure the existence of an effective judicial oversight mechanism (court permission), as

[272] "What's the News on the Wiretapping Bill?" *Tempo.co,* June 26, 2021 https://www.tempo.co/ Hukum /apa-kabar-ruu-denganadapan -823459. Accessed on November 2025

well as the affirmation of limitations and supervision to prevent unauthorized wiretapping or accountability for its use.

On the other hand, technical details related to the use and procurement of spyware are not clearly and comprehensively stated in publicly available laws. Frequently encountered practices are usually regulated by internal institutional regulations, with limited public access. However, legal prohibitions on wiretapping and interception of communications are regulated through legislation. For example, Article 31 of the ITE Law (Law No. 11/2008 jo. amendments) prohibits unauthorized interception and sets legal limits on the practice. Constitutional Court (MK) Decision No. 5/PUU-VIII/2010 stated that wiretapping is a highly sensitive matter because it restricts human rights and must be regulated by a specific law. The follow-up to this decision was only regulated by a Government Regulation (PP), which subsequently sparked controversy because it was deemed unable to meet the requirements of legality, transparency, and the need for regulation by law.[273] Therefore, this regulatory vacuum can provide input for the government and legislation to create more comprehensive regulations on wiretapping and spyware as separate normative objects.

No official evidence that Indonesia purchased Pegasus has been found. However, reports from Citizen Lab and Amnesty Tech between 2019 and 2021 confirm traces of the spyware infection on devices belonging to several activists and journalists in Indonesia. If procurement did occur, it likely involved the State Intelligence Agency (BIN) or Densus 88, was conducted off-budget (outside the formal state budget), involved secret purchases, and did not go through standard procurement mechanisms such as the Electronic Procurement Service (LPSE) through tenders. There is evidence of the import and use of surveillance technology through intermediaries and non-public commercial channels. Investigative reports and media coverage have documented traces of products like Pegasus and other spyware entering Indonesia, and there have been findings

[273] Nur Alam, "The Constitutionality of Wiretapping (Interception) with Government Regulations from the Perspective of Human Rights Protection," *Jatiswara* 27, no. 3 (November 2012).

of acquisitions through third parties or intermediaries.[274] While the procurement of spyware is beneficial for combating crime, its use is highly susceptible to abuse, and spyware itself has become a global human rights and security issue.

The traces of spyware use in Indonesia were uncovered in a collaborative investigation between Amnesty International and Tempo. The investigation revealed that from 2017 to 2023, several state institutions and companies in Indonesia were suspected of importing and using spyware technology. The report also identified that these surveillance devices were not supplied directly, but rather through a complex network of intermediaries and brokers. This distribution pattern resulted in transactions and use of these devices being secretive and non-transparent. Four vendors were identified, including Luxembourg-based Q Cyber Technologies SARL (associated with the NSO Group), a consortium of Intellexa, Wintego Systems Ltd, and Israel-based Saito Tech (then known as Candiru), and Malaysia-based Raedarius M8 Sdn Bhd (associated with FinFisher). The spyware devices entering Indonesia were allegedly purchased and used by institutions such as the Indonesian National Police and the National Cyber and Crypto Agency (BSSN). This raises concerns about potential privacy violations and the shrinking of civic space, particularly given the lack of clear regulations governing the use of spyware surveillance technology in Indonesia.[275] Furthermore, an Amnesty International report strongly alleges the involvement of a network of domestic and international companies in the procurement of sophisticated surveillance technology for several state institutions in Indonesia.[276]

In Indonesia's evolving digital landscape, the dark shadow of spyware technology must be a serious concern due to its links to privacy vulnerabilities

[274] M. Faiz Zaki, "Amnesty International Reveals Police Imported Wiretapping Devices, Here's What Police Experts Say About Wiretapping Standard Operating Procedures," *Tempo.co,* June 20, 2024 https://www.tempo.co/ Hukum/amnesty- international-besar-polri-impor-alat-sadap-ini-kata-pakar-kepolisian-soal-sop-denganadapan -61122. Accessed on August 2025.

[275] Han Revanda Putra, "Tempo Investigation Reveals Israeli Company Suspected of Supplying Spyware to Indonesia Since 2017," *Tempo.co,* 20 June 2024 https://www.tempo.co/arsip/investigasi-tempo-besar-kompasi-israel-diduga-pasok-spyware-ke-indonesia-sejak-2017-62228 . Accessed on December 2025.

[276] Putra, "Tempo Investigation Reveals Israeli Company Suspected of Supplying Spyware to Indonesia Since 2017."

and national cybersecurity. Spyware procurement in Indonesia involves both state and non-state actors, such as private companies and others. Increasingly sophisticated spyware devices are now being used to target a wide range of targets, from activists to political figures. Although its procurement and use are often disguised under the pretext of national security and law enforcement, this practice still requires strict oversight.

I.2. Transparency Gaps in the Procurement of Goods and Services for Intelligence and Surveillance Technology

Allegations that Indonesian state institutions are using spyware are not new. Evidence of such use has appeared since 2013, in an official statement from the Ministry of Defense regarding the procurement of surveillance equipment. The Ministry of Defense stated that it had collaborated with a company called Gamma TSE Ltd. UK to procure anti-wiretapping equipment for use by the State Intelligence Agency (BIN). Furthermore, in 2018, the public was shocked by the use of the Pegasus spyware by the Indonesian National Police and BIN. Furthermore, this year, the Attorney General's Office (AGO) signed a cooperation agreement with telecommunications operators such as XL, Telkomsel, and others, granting the AGO extensive authority to install and operate wiretapping devices to obtain information for law enforcement purposes.[277]

Furthermore, the state budget for defense and security has seen a significant increase during the Prabowo Subianto administration. In 2025, the defense and security budget will increase by approximately IDR 25 trillion compared to 2024, from IDR 139 trillion in 2024 to IDR 165 trillion in 2025. The increase will primarily be aimed at improving the welfare of Indonesian National Armed Forces (TNI) soldiers and modernizing the country's primary weapons

[277] See, Fahmi Ramadhan, "Teken Nota Kesepakatan dengan Provider, Kejagung Bisa Pasang Alat Sadap untuk Kumpulkan Data," *Tribunnews.com,* 26 June 2025, https://www.tribunnews.com/nasional/2025/06/26/teken-nota-kesepakatan-dengan-provider-kejagung-bisa-pasang-alat-sadap-untuk-kumpulkan-data .

systems.[278] Furthermore, the estimated cost allocation for purchasing Pegasus spyware between 2016 and 2022 can be seen in the following table:[279]

Component	Estimated costs
Initial license fee (setup)	USD 8-10 million
Package per target (per device)	USD 500 thousand – 1 million per 10-50 targets
Annual technical support & maintenance	USD 1-2 million per year
Total contract (for 2–3 years)	USD 15-25 million (Rp250-400 billion)

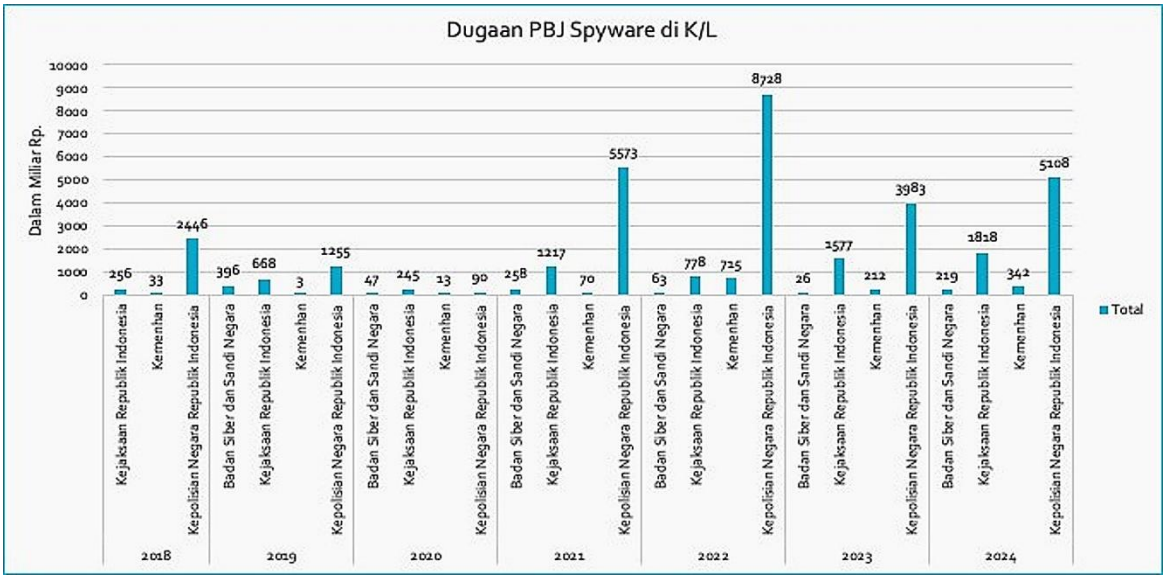
Furthermore, public spending on intelligence allocations, surveillance systems, and technology is a crucial component of the nation's law enforcement, security, and defense functions. This budget encompasses not only operational costs for personnel and logistics, but also the procurement of equipment and technological systems that support intelligence and surveillance functions. For example, in the 2018–2024 period, the Ministry of Defense (BIN) spent IDR 1.3 trillion on nine procurement packages related to digital activities, including command and control systems and intelligence target surveillance, indicating investment in monitoring and surveillance technology.

According to data from the National Secretariat of the Indonesian Forum for Budget Transparency (Seknas FITRA) and the Institute for Policy Research and Advocacy (ELSAM), five state institutions—the Indonesian National Armed Forces (TNI), the Indonesian National Police (Polri), the State Intelligence Agency (BIN), and the Attorney General's Office—spent IDR 36.1 trillion in the state budget on

[278] Kurnia Yunita Rahayu and Hidayat Salam, "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun," *Kompas.id*, 16 August 2024. https://www.kompas.id/article/sejalan-dengan-visi-prabowo-anggaran-perlahan-naik-jadi-rp-165-triliun . Accessed on 15 January 2026.
[279] Amnesty International report processed by FITRA

mass surveillance technology procurement. The budget allocation for intelligence and surveillance equipment across these four institutions from 2018 to 2024 can be seen in the diagram below.[280]

Alleged Procurement of Goods/Services for mass surveillance equipment



This analysis is reinforced by GlobalData's latest report, Indonesia Defense Market Size, Trends, Budget Allocation, Regulations, Acquisitions, Competitive Landscape and Forecast to 2030. The report reveals that Indonesia's cumulative defense spending is estimated to reach USR 46.6 billion in the 2024–2028 period. Of this total, the portion for the acquisition budget is predicted to be 28.4% or equivalent to USD 13.3 billion. Defense procurement spending is expected to record a compound annual growth rate (CAGR) of 1.5% during the 2024–2028 period and reach SD 2.7 billion in 2028. According to Abhijit Apsingikar, Aerospace & Defense Analyst at GlobalData, Indonesia's defense budget is largely driven by the need to mitigate the impact of natural disasters and undertake military modernization initiatives. Indonesia is seeking to expand its defense posture and

[280] FITRA processed data

enhance its domestic defense manufacturing industrial complex through military modernization initiatives. Furthermore, the rise in fundamentalism coupled with online radicalism has exacerbated the threat of terrorism, which, has forced Indonesia to invest heavily in cybersecurity and counter-terrorism apparatus.[281]

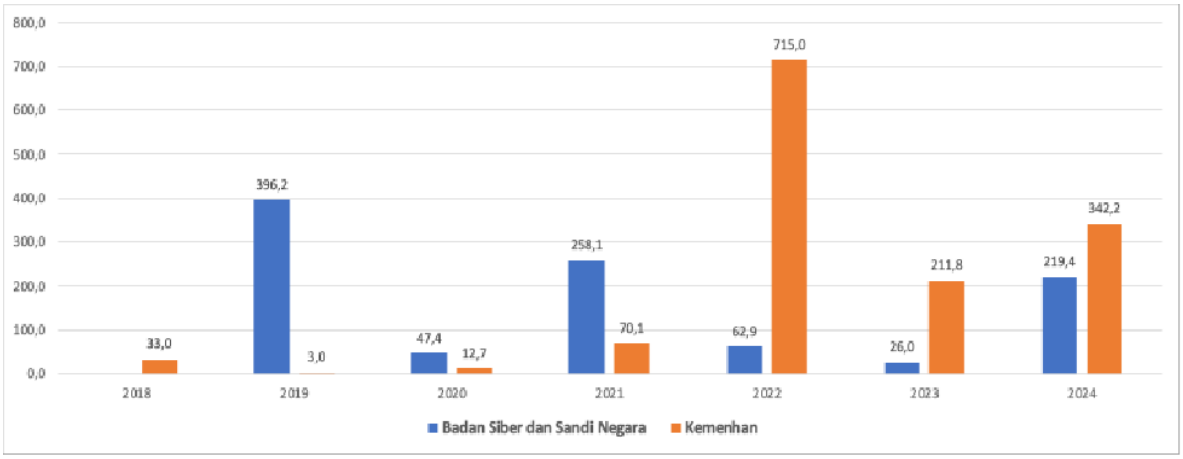
Internal budget data from law enforcement agencies and other government agencies also show significant funding allocated for intelligence equipment and surveillance devices. The Attorney General's Office budget document lists a budget ceiling of IDR 6.5 trillion for the procurement of intelligence equipment, digital forensic laboratories, and even tactical monitoring devices, all related to strengthening investigative and surveillance functions. Meanwhile, the National Cyber and Crypto Agency (BSSN), as the national cybersecurity authority for 2018-2024, received an indicative budget of approximately IDR 1 trillion. No budget was allocated for expanding surveillance coverage through the National Security Operation Center (NSOC), despite this being a priority program to improve cyber threat detection and response capabilities. This budget limitation is feared to impact the effectiveness of national cyberspace security. At the legislative level, members of the House of Representatives (DPR) also emphasized the importance of investing in modern intelligence technology to enhance the capacity of the State Intelligence Agency (BIN) to address increasingly complex security challenges in the digital era. According to Commission III member Bambang Soesatyo, the need for the latest intelligence equipment is part of efforts to safeguard national sovereignty and security.[282] The budget allocation for intelligence and surveillance tools at the Ministry of Defense can be seen in the chart below.[283]

---

[281] "Indonesia Defense Expenditure to Reach $9.7 Billion by 2028," *Asia Pacific Defense Reporter,* 31 August 2023, https://asiapacificdefencereporter.com/indonesia-defense-expenditure-to-reach-9-7-billion-by-2028/ . Accessed on 15 January 2025.

[282] Bagus Ahmad Rizaldi, "Anggota DPR Sebut BIN Perlu Investasi Teknologi Intelijen Terkini," *Antaranews.com*, 21 May 2025, https://www.antaranews.com/berita/4820745/Member-dpr-buat-bin-perlu-investasi-technology-intelijen-terkini . Accessed on December 2025.

[283] FITRA processed data



The issue of transparency and accountability in budgets for the procurement of surveillance technology often comes under scrutiny from the public and civil society organizations. Concerns arise especially when large budgets are allocated to sensitive systems such as digital surveillance and surveillance capabilities without detailed public explanation of their objectives, oversight mechanisms, and guarantees of human rights protection. Large budgets for listening devices are often unaccompanied by evidence of effectiveness and robust control mechanisms, so the potential for misuse cannot be ignored.[284] From a public budget policy perspective, spending on intelligence and surveillance is indeed a strategic necessity in maintaining national security. However, allocations for intelligence and surveillance also require a strict internal oversight system, transparency in budget use, and a clear legal framework to prevent these functions from violating privacy rights or fundamental civil liberties, both in the digital and physical space.

If examined further, there are ten major procurements of goods and services for intelligence and surveillance equipment throughout 2018–2024, as seen in the table below.[285]

[284] Alliance of Independent Journalists, "Jelang Pemilu 2024, Perlu Regulasi Penggunaan Alat Sadap seperti Pegasus," *Aji.or.id*, 23 June 2023. https://www.aji.or.id/information/jelang-pemilu-2024-perlu-regulat-useran-alat-sadap-cepat-pegasus . Accessed on December 2025.

[285] FITRA processed data

Year	Intelligence and Surveillance Tools	Ministry	Budget	Selection Method
2021	Procurement of Information Technology Surveillance System Equipment (Active)	Indonesian Attorney General's Office (Kejagung)	488,469,587,460	Direct Purchase
2023	Dynamic Active Target Monitoring System Combat Equipment	Indonesian National Police (Polri)	418,849,966,000	Direct Purchase
2022	Procurement of Hybrid Surveillance Car with Compact Portable Active Intelligent Intercept FY 2022	Polri	412,644,600,000	Tender
2023	Procurement of Surveillance Car with Active Intercept Monitoring Intelligence System	Polri	399,716,120,000	Tender
2019	Procurement of Counter Surveillance Equipment Phase III	Kejagung	379,782,040,000	Direct Purchase
2022	Procurement of Hybrid Surveillance Car with Compact Portable Active Intelligent Intercept FY 2022	Polri	359,805,343,000	Tender
2022	Procurement of Disclosure Mobile Surveillance and Communication Devices Detector FY 2022	Polri	352,484,407,000	Tender
2022	Procurement of Disclosure Mobile Surveillance and	Polri	352,484,407,000	Tender

	Communication Devices Detector FY 2022			
2023	Procurement of Hybrid Surveillance Car with Compact Portable Active Intelligent Intercept	Polri	350,138,916,000	Tender
2024	Procurement of Biometric-Based Digital ICT Card Intelligence Equipment for the Indonesian Attorney General's Office's Criminal Data	Kejagung	350,000,000,000	Direct Purchase

Furthermore, the allocation of the top ten procurement of goods and services in the Ministry of Defense throughout 2018-2024 can be seen in the following table.[286]

Year	Intelligence and Surveillance Tools	Work Unit	Budget	Selection Method
2022	Intelligence Cyber Command System	Indonesian Army Headquarters	199,995,537,000	Direct Purchase
2024	Procurement of Threat Intelligence and Target Intelligence Monitoring System (Dispamsanal)	Indonesian Navy Headquarters	100,000,000,000	Direct Purchase
2022	Portable Wireless Intelligence Monitoring System	Indonesian Army Headquarters	97,348,807,000	Direct Purchase

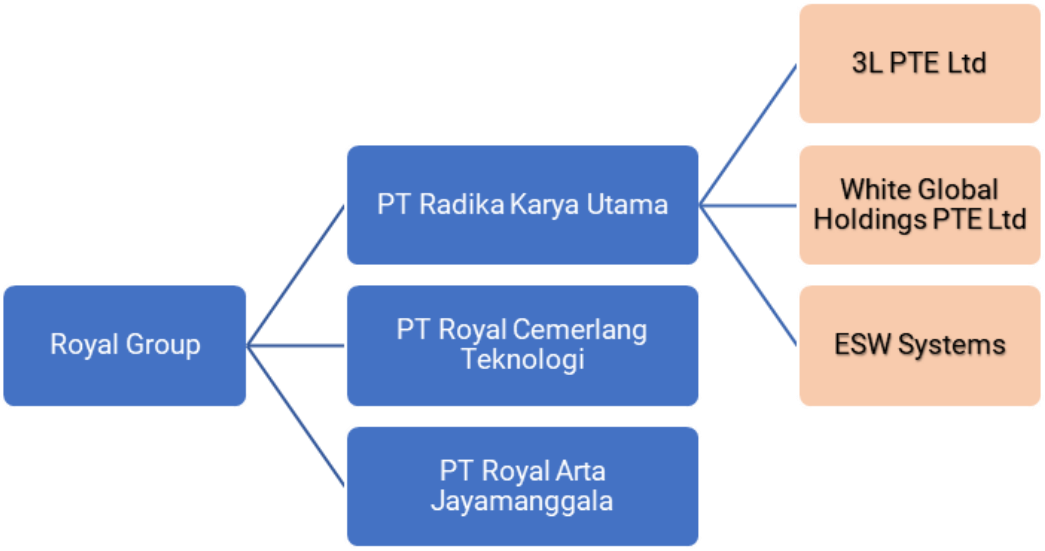
[286] FITRA processed data

2022	Stealth Intelligence Military Task	Indonesian Army Headquarters	97,155,441,000	Direct Purchase
2022	Baseline Electronic Aggregation Cyber Center	Indonesian Army Headquarters	96,218,126,000	Direct Purchase
2022	Locator Intelligence Information Control of Dissemination Area	Indonesian Army Headquarters	95,020,118,000	Direct Purchase
2024	Cyber Troops System Procurement (Multiyear Phase II)	Indonesian Army Headquarters	69,993,498,000	Direct Purchase
2024	Procurement of Integrated Wireless Intelligence Secure Data (Multiyear Phase II)	Indonesian Army Headquarters	67,846,877,000	Direct Purchase
2024	Silent Intelligence Tap Wire Procurement (Multiyear Phase II)		59,311,174,000	Direct Purchase
2023	Tactical Intelligence Monitoring Surveillance Phase I	Indonesian Army Headquarters	43,500,000,000	Direct Purchase

Based on the data above, procurement budgets for goods and services for intelligence, surveillance, and spyware technology in Indonesia are often allocated through direct purchase mechanism. The use of this mechanism is often based on considerations of confidentiality, security urgency, the strategic nature of the activity, and even vendor limitations. Regulatory requirements allow

for this scheme within government procurement regulations. However, in practice, direct purchase is often used for high-value, high-risk surveillance technology procurements without an adequate competitive process.

This situation is reinforced by an Amnesty International report that reveals a network of domestic and international companies procuring advanced surveillance technology for state institutions in Indonesia. One of the main actors in the procurement of spyware devices in Indonesia is PT. Radika Karya Utama, an Indonesia-based company with a history of procuring surveillance technology on behalf of government institutions, in addition to other commercial activities not directly related to surveillance systems. PT. Radika Karya Utama also operates through a number of other corporate entities, such as PT. Royal Cemerlang Teknologi and PT. Royal Arta Jaya Manggala, which are often linked under a single business umbrella known as the Royal Group. The Royal Group's organizational structure network in procuring spyware devices in Indonesia can be illustrated in the following figure:[287]



Based on public tender documents, it is known that PT. Radika Karya Utama

[287] Amnesty International, "A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia." https://www.amnesty.org/en/documents/asa21/7974/2024/en/ Accessed on December 2025.

once won the procurement of a zero-click intrusion system and has a telecommunications surveillance and geolocation system originating from Circles, an affiliate of the Israeli NSO Group. The system was reportedly implemented on the IP networks 203.142.69.82-84 and 117.102.125.50-52 registered in the names of these companies. PT Radika Karya Utama's tender documents indicate direct involvement in the implementation of advanced surveillance technology.[288]

Skor	Judul	Penyedia	LPSE	Tanggal Pengumuman	Nilai Kontrak
50	PERALATAN DAN MATERIIL KHUSUS DIT INTELKAM (ZERO CLICK INSTRUKSION SYSTEM) POLDA METRO JAYA BERIKUT PENGIRIMAN	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	22 September 2017	Rp 98.912.000.000,00
57	PENGADAAN ALMATSUS PENGEMBANGAN ZERO CLICK INSTRUSION SYSTEM (IOS) APBN TA. 2018	PT. RADIKA KARYA UTAMA	LPSE Kepolisian Republik Indonesia	14 February 2018	Rp 149.831.000.000,00

At the international level, Amnesty International also identified the roles of White Global Holdings PTE Ltd, 3L PTE Ltd, and ESW Systems. These three Singapore-based companies portray themselves as interconnected entities active in the trade of surveillance technology and military and police equipment for the global market, including Indonesia. The ownership structures of these three companies are considered opaque. Corporate records reveal that several Indonesian citizens have been listed as shareholders and administrators, including individuals with ties to Indonesian companies. Trade records show that in March 2019, White Global Holdings shipped a product described as an "Android one-click installation module " to the National Cyber and Crypto Agency (BSSN). This description indicates the sale of a spyware solution capable of directly infecting target Android devices. Furthermore, in July 2021, ESW Systems was recorded as exporting various surveillance system licenses worth over USD 11 million to the Indonesian National Police, including licenses for watchlist-based graphical detection and real-time geolocation tracking systems. These products

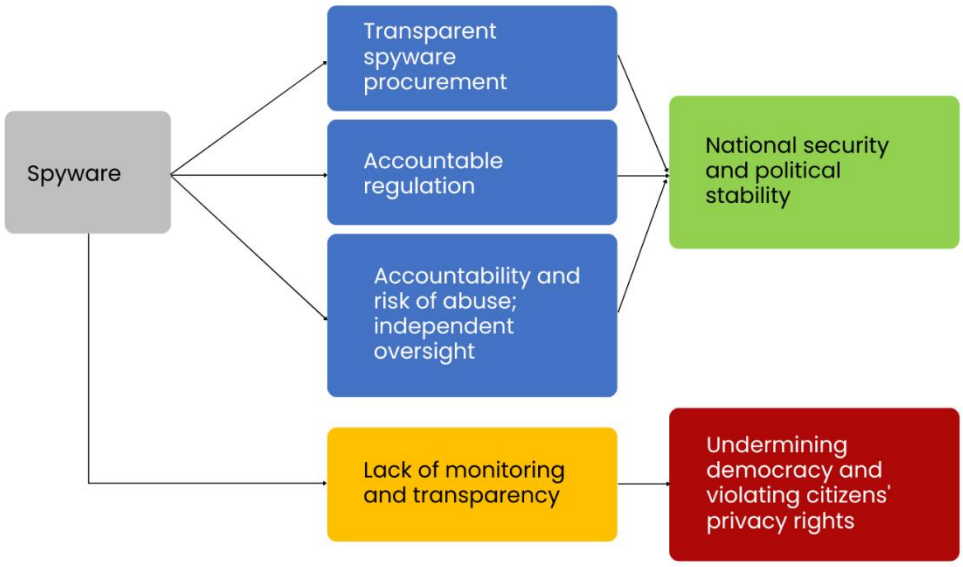
[288] See *OpenTender.net*

are suspected of being related to cellular network traffic analysis and surveillance-based tracking systems. Other trade records also show shipments of a product labeled "WINT SYSTEM" from ESW Systems to the Indonesian National Police, believed to be related to surveillance technology from Wintego Systems, a company known for marketing spyware and tactical network interception. All of these products fall into the category of dual-purpose technologies that have the potential to be used as instruments for human rights abuses.

Amnesty International contacted all of the companies mentioned, including Radika, White Global Holdings, 3L, ESW Systems, and Royal Group entities, to request clarification regarding the procurement of spyware, inter-company relationships, and compliance with human rights commitments under the UN Guiding Principles on Business and Human Rights. However, none responded before the report was published. Clarification requests were also submitted to the Indonesian National Police (Polri) and the National Cyber and Crypto Agency (BSSN), but received no substantive response. The Indonesian National Police declined to respond to the allegations. Furthermore, Amnesty International also revealed the involvement of HEHA, a Singapore-based company, which exported hardware dubbed the "Cyber Intelligence Infiltration; Exfiltration System" to the Indonesian National Police in 2020–2021 with a total value of approximately USD 33 million. Like the other companies highlighted, HEHA did not provide clarification on questions regarding its technology manufacturer, procurement mechanisms, or human rights impact assessment. These findings highlight the lack of transparency and accountability in the procurement of surveillance technology in Indonesia, as well as the potential for spyware misuse amid the absence of a comprehensive legal framework to regulate digital wiretapping and surveillance practices.

The opaque and minimally accountable trade in spyware into Indonesia has added to the growing list of dangerous tools potentially used for intimidation. An investigation by Amnesty International's Security Lab uncovered evidence of the sale and distribution of invasive spyware to several state institutions, including the Indonesian National Police (Polri) and the National Cyber and Cyber Security

Agency (BSSN), between 2017 and 2023. These transactions occurred through a network of vendors and brokers operating with complex ownership structures and minimal transparency, including Q Cyber Technologies (NSO Group), Intellexa, Wintego, Candiru, and Raedarius M8 (FinFisher). The investigation also identified a malicious digital infrastructure associated with Intellexa's Candiru and Predator spyware. This infrastructure included the use of fake domains designed to trick journalists, civil society organizations, and even opposition parties into clicking on malicious links that could potentially infect their devices. While evidence of direct infection of specific individuals is difficult to establish due to the highly classified nature of spyware, the existence of this infrastructure confirms the existence of systematic targeting efforts.[289] The impact of using spyware devices, if no arrangements are made to demand accountability based on human rights, the rule of law, and justice, can be seen through the illustration in the image below.[290]



This situation indicates a pattern of repeated direct purchases involving the same providers in the procurement of intrusion systems, geolocation tracking, and digital monitoring devices. The lack of public disclosure of technical specifications, contract values, and the basis for selecting these providers raises

[289] Amnesty International, "A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia."
[290] Figure processed by researchers

serious concerns about potential conflicts of interest, budget inefficiencies, and misuse of surveillance technology. This situation highlights the gray area between state security needs and the principle of public budget accountability. Without strict oversight, human rights due diligence, and independent oversight mechanisms, the practice of direct appointments in surveillance technology procurement risks weakening budget transparency and increasing threats to citizens' privacy rights and fundamental civil liberties. At the same time, procurement of spyware-related goods and services in Indonesia faces serious accountability challenges, particularly due to the sensitive nature of this technology and its potential for misuse. Therefore, export controls on espionage technology and increased transparency and accountability in its use are needed to protect the fundamental rights and freedoms of every citizen.

I.3. Traces of Spyware Use in Indonesia and Its Threats to Human Rights: Case Reflections

Core Developers and Support Networks

In a 2024 report published by Amnesty International titled "Global: A Web of Surveillance – Unraveling a Murky Network of Spyware Exports to Indonesia," at least five spyware companies are identified to have sold their technology to Indonesia: FinFisher, Wintego Systems Ltd, Intellexa Consortium, Candiru, and NSO Group. These spyware products are suspected of being used by various institutions, including the State Intelligence Agency (BIN), the National Security Agency (BSSN), the Indonesian National Police (Polri), and the Indonesian National Armed Forces (TNI). The following are the details of the five companies:

1) Finfisher

Finfisher is a tool developed by Gamma International GmbH from Munich, Germany, that functions as an intrusion and remote monitoring tool. The tool is then marketed and sold by the UK-based Gamma Group to law enforcement and state intelligence agencies.[291] The FinSpy marketing brochure explains that this

[291] Morgan Marquis-Boire et al., "You Only Click Twice: FinFisher's Global Proliferation," *Citizen Lab,* March 13, 2013, https://citizenlab.ca/research/you-only-click-twice-finfishers-global-proliferation-2/#1 .

technology works by penetrating 40 regularly tested antivirus systems, communicating with the main office, and being able to monitor Skype activity (calls, messages, file transfers, videos, and contact lists). In addition, this technology can record various forms of common communication such as email, instant messages, Voice-Over-IP, perform live monitoring via webcam and microphone, track the target's country of origin, secretly extract files from the hard disk, record keyloggers to speed up analysis, perform remote forensics directly on the target system and apply filters to information deemed important. This technology can work on various Windows, Mac OS X, and Linux devices. Once this tool is installed, the infected device can be accessed and controlled remotely as long as the system is connected to the internet, regardless of the target's geographic location.[292]

In 2012, Citizen Lab monitored FinSpy servers for a year and discovered 36 FinSpy servers spread across 25 countries, including Indonesia, Australia, Bahrain, Bangladesh, Brunei, Canada, the Czech Republic, Estonia, Ethiopia, Germany, India, and others. In Indonesia, the technology has been operational since 2012, and three telecommunications operators have been identified as using the technology from Gamma International GmbH: PT Telkom, PT Matrixnet Global, and Biznet ISP. Internet Protocol (IP) addresses are intentionally not fully publicized to prevent operators from disabling or moving their server infrastructure during the monitoring process. However, the table below summarizes a number of IP addresses that have been strongly identified as using FinSpy technology in Indonesia.

IP Address	Operator	Country
118.97.xxx.xxx	PT Telkom	Indonesia
118.97.xxx.xxx	PT Telkom	Indonesia
103.28.xxx.xxx	PT Matrixnet Global	Indonesia

[292] https://wikileaks.org/spyfiles/docs/gamma/289_remote-monitoring-and-infection-solutions-finspy.html

112.78.143.34	Biznet ISP	Indonesia
112.78.143.26	Biznet ISP	Indonesia

In addition to being used by telecommunications operators, FinSpy technology is also suspected of being used by a state institution, namely the National Cyber and Crypto Agency (BSSN). This indication first emerged when a Hacking Team member was in Indonesia to conduct a technology trial for BSSN. The IP address associated with FinSpy, "/28," as found in various countries such as Mongolia, Belgium, and Serbia, was also found in the header of an email sent by the Hacking Team employee while he was at BSSN.[293] The email was sent at 12:39 West Indonesian Time on 6 February 2013, and on the same day, a meeting had been scheduled for 10:00 WIB at the agency. Based on these findings, it is highly likely that the email was sent from within the BSSN building, and the two FinFisher servers located within the same IP address block are likely also owned or operated by the organization.

In the context of import and export, Gamma International GmbH does not directly sell FinSpy products to Indonesia, but rather through a business entity called Raedarius M8 located in Malaysia and Germany. Then, it is sold to Indonesia in the form of hardware components such as Fanless Computer Accessories, Plastic Cases, Power Supplies for Single Board Computers, and so on to PT. Digital Solusi Prima, an Indonesian company, of course at a fantastic price. However, there are no further findings regarding who these products are sold to.[294] It is important to note that spyware is not always sold as a complete product. In many cases, this technology is offered in the form of separate components that are then assembled, customized, or integrated by the buyer in Indonesia.

[293] Bill Marczak et al., "Mapping FinFisher's Continuing Proliferation," *Citizen Lab,* October 15, 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#51 .
[294] Amnesty International, "A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia."

2) Wintego Systems Ltd

Wintego Systems Ltd is a company that sells Israeli surveillance software to the Indonesian National Police through retail companies in Singapore called Ataka Enterprises Pte Ltd and ESW Systems Pte Ltd.

The products offered include Helios, a Catch App operating under the WINT brand, which is used to penetrate WhatsApp encryption and collect all data such as messages, voice recordings, documents, photos, and other data sent or received by other WhatsApp users. In addition to WhatsApp, in 2022, the software was discovered to be able to remotely infiltrate Android phones using the Chrome and Samsung browsers.

Furthermore, this one-click intrusion system spyware operates by impersonating legitimate news portals or websites. Based on a 2018 network analysis conducted by Amnesty International on the tribunnews.org website, it was discovered that the spyware impersonated the TribunNews.com news portal. Another site that was impersonated was galaxyupdate(.)network, a Samsung mobile phone domain. Once the site is accessed by the victim, the spyware automatically infects the victim's device.

After analyzing the commercial trade database, it was discovered that Wintego products were sold to Indonesia on 9 September 2019, through a company called ESW Systems located in Singapore, directly to the Indonesian National Police.

3) Intellexa Consortium

Intellexa Group is a company founded in 2018 by an Israeli military officer named Tal Dilian and other colleagues. Its products include tactical and zero-click network injection. The company then evolved into a consortium. Shareholders in the Intellexa Consortium include Wispear (Cyprus), Cytrox (North Macedonia), Cytrox Holdings Zrt (Hungary), and Intellexa SA and Thalestris Ltd

(Ireland).[295] Most of these companies specialize in Open Source Intelligence (OSINT) and virtual avatar creation.

Intellexa Alliance's spyware, known as Predator, is a highly intrusive piece of spyware. It can access all data stored and transmitted on a victim's device and is designed to leave no trace on the device, making it impossible to prove any actual or potential misuse of the spyware.

Following a recent IP address search of fake websites impersonating the official Suara Oposisi (Opposition Voice), Gelora News (a website belonging to the Gelora Party), and Suara Papua, Amnesty International discovered that spyware technology called Predator had been in use in Indonesia since 2021 and had been in use for at least two years until December 2023.[296]

In addition to Predator, Intellexa Group also owns various technologies and supporting components used to build and operate the spyware ecosystem. These technologies include Helios, Green Arrow, Red Arrow, CyOP, AAA, SpearHead, Alpha-Max, Epsilon, PDS, Nebula, IS, Nova, Triton, Mars, Jupiter, Orion, Cerebro, Jasmine, IOTA, Eagle, GLINT, and SMINT, each with distinct functions.[297]

These components are designed to support a wide range of surveillance needs, from spyware capable of intruding into a target's digital device, the main supporting component of Predator, interception analysis tools, avatar or bot systems to manage "avatars," which are fake accounts on social media and messaging apps, used to social engineer targets into opening one-click links, to Internet Traffic Monitoring. This approach allows Intellexa to build a flexible surveillance system, adaptable to the needs of operators/users, and integrated into a complex and coordinated surveillance ecosystem.

[295] Amnesty International Security Lab, "Technical Deep Dive into Intellexa Alliance Surveillance Products," *Amnesty International,* 9 October 2023, https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/ .
[296] Amnesty International, "Technical Deep Dive into Intellexa Alliance Surveillance Products."
[297] Amnesty International, "Technical Deep Dive into Intellexa Alliance Surveillance Products."

4) Candiru/ Saito Tech

Candiru, commonly known as Saito Tech, is a surveillance company that develops and sells a cyber infiltration system called Cyrus, which is used to infiltrate devices such as Windows PCs, Android, and iOS. The company was founded in 2014 by Ya'acov Weitzman and Eran Shorer, both of whom have a history as members of the IDF Military Intelligence Unit 8200 and previously worked at the NSO Group, widely known for its spyware product, Pegasus.[298]

Amnesty International and Citizen Lab's findings indicate that the product entered Indonesia through a Singapore-based company, Heha Pte Ltd, for use by the Indonesian National Police. This device is known to have been in use since 2020. The product exported to Indonesia was shipped in the form of several separate hardware components, which included a management server, visualization server, central storage, backup server, switch, UPS, firewall, KVM with display, and server rack. The shipment was carried out in two stages, namely in May 2020 with a value of USD 79,303, and in July 2020 with a value of USD 75,815.[299] In 2021, it was discovered that there was a separate procurement on 27 January 2021, related to software components and licenses worth USD 33,089,849.

Similar to the Wintego Systems Ltd. tool, the Candiru/Saito Tech product works by impersonating the official websites of TribunNews, Tirto, MediaIndonesia, ANTARA News, Indoprogess, and the Gelora Party. This technology is not only operational in Indonesia, but also in Saudi Arabia, Israel, the UAE, and Hungary.

5) NSO Group

NSO Group is named for the acronym of its founders, Niv Carmi, Shalev Hulio, and Omri Lavie. This company is an Israeli spyware company that develops cyber surveillance software capable of infiltrating personal devices running operating systems like iOS and Android. In addition to operating as the main entity, the

[298] Sophie in 't Veld (Rapporteur), *Draft Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI)),* European Parliament Committee of Inquiry (PEGA), 8 November 2022.
[299] Amnesty International, "A Web of Surveillance: Unraveling a Murky Network of Spyware Exports to Indonesia."

company also has several subsidiaries, including Circles and Q Cyber Technologies.

A forensic report issued by Amnesty International, Citizen Lab, and several other organizations indicates that at least 12 countries use or procure spyware technology from NSO Group. These include Germany, the United Kingdom, Switzerland, France, the United States, and Indonesia.[300] A shipment from Q Cyber Technologies to an Indonesian company was discovered. In 2023, Tempo, a member of the Indonesian Leaks network, revealed that Pegasus technology was allegedly used by the Indonesian National Police and the State Intelligence Agency (BIN).

According to data from the Indonesian National Police's Electronic Procurement Service (LPSE), the tender was won by an Indonesian company named PT Radika Karya Utama. The technology in question was listed under the name "Zero Click Intrusion System DIT Intelkam Special Material Equipment" and was included in two procurements, one in September 2017 and one in February 2018, with a total value of approximately IDR 247.7 billion.

The involvement of the five major vendors mentioned above is just one part of a more complex surveillance ecosystem in Indonesia. Beyond these intrusion software providers, further investigation revealed a network of supporting entities and intermediaries that play a role in providing operational infrastructure and complementary technologies. A corporate affiliation investigation conducted by FIND in November 2025 expanded this map by identifying three additional entities closely linked to the country's surveillance technology supply chain. These entities are Polus Group, Therian Lab, and Pallabotta Technologies Ltd.

Polus Group, also known as Polus Tech, is a Swiss-based surveillance technology company. It was founded by Niv Karmi, a well-known figure in the global surveillance technology industry, being a co-founder of NSO Group, the

[300] Amnesty International Security Lab, "Forensic Methodology Report: How to Catch NSO Group's Pegasus," *Amnesty International,* 18 July 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/ .

controversial spyware company that has drawn international attention.

Polus Group itself focuses on the development and distribution of surveillance technology, especially technology that has the ability to intercept and monitor communications via mobile phone devices, one of which is a technology known as IMSI Catcher.

An IMSI Catcher is a technology device designed to monitor and identify mobile devices over a cellular telecommunications network. It works by mimicking the signal of a mobile phone base transceiver station (BTS), so that nearby mobile devices automatically connect to it. Through this mechanism, an IMSI Catcher can capture the entire unique identification number (International Mobile Subscriber Identity/IMSI) of every mobile phone within its range without the device owner's knowledge.[301]

Through a corporate affiliation search of individuals connected to the Polus Group as of 18 November 2025, FIND identified several entities domiciled in Singapore, Cyprus, and the United Arab Emirates. These entities, between 2023 and 2025, distributed surveillance technology through several schemes, namely (1) to companies in Indonesia that had previously received similar products directly from the Polus Group; (2) to other identified government contractors in Indonesia; or (3) directly to Indonesian law enforcement agencies.

Niv Karmi's business network ties do not stop at Polus Group. He is also listed as a board member of Therian Labs Technologies AG, a separate entity engaged in a similar industrial ecosystem, namely the development and distribution of military signal intelligence products for public security and homeland security purposes. Therian Labs itself has a board member and sole shareholder named Itiel Elata, this is proven by the existence of an official email address with the Polus Group domain, namely itiel.elata@polustech.com and is known to be still active until 19 September 2025. In addition, he is known to have attended the Indo Defence Expo and Forum in Jakarta, Indonesia in June 2025 in his capacity as an

[301] Privacy International and ELSAM Team, *Privacy 101: A Guide to Understanding Privacy, Data Protection, and Communications Surveillance,* (Jakarta: ELSAM, 2015), p. 45-46.

Executive of Polus Tech (Switzerland) Ltd.

The company obtained an export license for surveillance technology to Indonesia in 2022, valued at CHF 4.84 million, equivalent to IDR 75.3 billion (based on the 2022 average exchange rate). However, to date, no international trade aggregate data has been found that explicitly lists Therian Labs as the shipper or consignee in any shipment.

The complexity of Itiel Elata's business network became even more apparent when it was discovered that he had also served as Director of Pallabotta Technologies Ltd since July 2021. This company's presence adds a new layer to Elata's business affiliation network, which already includes Therian Labs. For the record, Pallabotta Technologies Ltd has an affiliate operating in Dubai, Pallabotta Technologies FZCO (hereinafter referred to as Pallabotta UAE). The presence of this entity expands the operational reach of the business network to the Middle East.

In a trade data aggregation, it was found that Pallabotta UAE had made 174 shipments to Indonesia from May 2023 to June 2025. The details are as follows:

a. In May 2023, 18 shipments were delivered to PT. Radika Karya Utama, comprising components, licenses, and programs related to the target location tracking system, worth USD 11,106,110. Then, in June 2025, two more shipments, a "Digital Forensic Toolkit" and a "Portable Active Monitoring System," were delivered, worth USD 2.5 million.

b. Several months later, in November 2023, there were 28 shipments of the same product, addressed to the Attorney General's Office, totaling USD 11,723,920.

c. Additionally, from February 2024 to May 2025, 126 shipments were shipped to PT Terra Lentera Asia. The products distributed by the company were described under various labels, including 'data analytics', 'strategic analysis investigation tools and target identification ', and 'intelligence equipment '. The total value was USD 62,245,180.

Additionally, Terra Lentera Asia won a closed tender held by the Attorney General's Office of the Republic of Indonesia on December 28, 2023, with a contract value of USD 12 million, equivalent to IDR 189.6 billion. The tender covered the procurement of surveillance capabilities, the description of which was almost word-for-word identical to the product specifications subsequently submitted by Pallabotta UAE to Terra Lentera Asia in February 2024.

The precise match between the tender documents and the delivery specifications is difficult to dismiss as mere coincidence, and instead strengthens the suspicion of a direct link between Pallabotta UAE's distribution network and the surveillance technology procurement contract obtained by Terra Lentera Asia from state law enforcement institutions.

These findings are even more concerning when compared with recent policy developments. On June 25, 2025, the Attorney General's Office of the Republic of Indonesia officially signed a Cooperation Agreement (PKS) with four national telecommunications operators: PT Telekomunikasi Indonesia Tbk, PT Telekomunikasi Selular, PT Indosat Tbk, and PT XLSmart Telecom Sejahtera Tbk. The agreement was officially based on the need to optimize the Attorney General's Office's intelligence function, particularly in tracking fugitives and managing the Wanted List (DPO).[302]

Spyware Technology Broker/Middleman Companies in Indonesia

This network structure is further layered with the involvement of a number of local intermediary companies that manage administrative and distribution aspects. Entities such as Radika Karya Utama, Terra Lentera Asia, and Maracipta Utama have emerged as key actors in this distribution chain. Their role as intermediaries not only facilitates access for foreign vendors but also widens the accountability gap in the procurement of intelligence technology goods and

[302] ELSAM (Institute for Research and Community Advocacy), "Kejaksaan Agung Teken MoU Penyadapan dengan Operator Telekomunikasi, Privasi Warga Dikorbankan atas Nama Penegakan Hukum," Press Release, 26 June 2025, Accessed on 28 March 2026, https://www.elsam.or.id/siaran-pers/kejaksaan-agung-teken-mou-penyadapan-dengan-operator-telekomunikasi--privasi-warga-dikorbankan-atas-nama-penegakan-hukum .

services in Indonesia.

PT. Radika Karya Utama (RKU) is an Indonesian company founded in 2007. This company's name is often mentioned in various reports related to the alleged procurement of surveillance technology with a very high level of intrusion in the form of Pegasus spyware produced by the NSO Group (Israel). This company's name first emerged in Amnesty International's findings, which indicated a link between entities in Indonesia with the distribution or supply chain of surveillance technology to the Indonesian National Police with a reported procurement value reaching IDR 247.7 billion in 2017-2018.

In addition to NSO Group products, based on our analysis of international trade data aggregation obtained from the FIND NGO,[303] we discovered a shipment of surveillance technology products from the Polus Group (Switzerland) to RKU in March 2021. In the shipping documents, the products shipped were disguised with the labels "Pelican Cases" and "Textile Rucksack", with a total recorded value of USD 950.

Several years earlier, in 2020, the Polus Group had obtained an export permit for surveillance equipment worth CHF 2.23 million, equivalent to IDR 48 billion. The following year, in 2021, the company was granted an additional export permit worth CHF 1.7 million, equivalent to IDR 36.6 billion.

Furthermore, in 2022, the Polus Group again obtained an export permit for surveillance equipment worth CHF 22.86 million, equivalent to IDR 355.6 billion (based on the 2022 average exchange rate of IDR 15,557/CHF). However, after that period, no evidence of direct shipments from the Polus Group to Indonesia was found. Subsequent shipments were made through an intermediary (middleman), a company identified as Radika Karya Utama.

IndonesiaLeaks found that RKU has allegedly procured various surveillance technologies, including a zero-click intrusion system, on behalf of the Indonesian National Police since at least September 2017. The Amnesty Tech report also

[303] FIND is a non-profit investigative organization focused on tracking the business networks and financial flows behind the deployment of surveillance technology. https://find.ngo/about

indicates that RKU may have acted as an intermediary seller for the NSO Group and its subsidiary, Circles. This indication is based on the discovery of technical infrastructure where the surveillance system allegedly used in Indonesia was detected operating on an IP address registered under the name "RADIKA KARTA UTAMA," which is very likely a misspelling of part of the company's name.

In addition, three other Singaporean companies, ESW Systems Pte Ltd, White Global Holdings, and 3L Pte Ltd, delivered surveillance equipment to RKU in November 2020 and June 2021, contemporaneously with the Polus Group shipment. To date, no connection has been identified between the shipments made by these three Singaporean companies and the Polus Group. FIND's brief findings indicate that in December 2020, several items were shipped to RKU, labeled "Nemesis Tactical Backpack," "Nemesis Enigma GSM Interception System," and "Nemesis Vehicular Mobile Targeting Surveillance System," worth $4 million. However, it is unknown to whom these items were ultimately sold.

Exactly ten months later, Polus Group was recorded shipping a product called the 'Nemesis B-Unit' to an Indonesian company, Maracipta Utama. What is striking is the significant similarity between the product shipped by the Singaporean company, 3L Pte Ltd, and the product shipped by Polus Group. This similarity raises suspicions that 3L Pte Ltd may be a subsidiary of Polus Group, or at least has a partnership with the company.

Politician Involvement in Spyware Procurement in Indonesia

A more surprising finding was revealed through a document notifying changes to the General Legal Administration (AHU) company data dated November 29, 2023, belonging to PT Radika Karya Utama, which ELSAM obtained from the Ministry of Law and Human Rights (Kemenkumham), a ministry that has now undergone a change in nomenclature to the Ministry of Law following the separation of human rights affairs under the administration of President Prabowo Subianto. The document explicitly lists the composition of the company's management and shareholders, and most astonishingly, one of its main commissioners is a politician who served as a member of the Indonesian House

of Representatives (DPR RI) for the 2014–2019 period.[304]

This fact is not simply an administrative anomaly. The presence of politically motivated figures within the core structure of a company suspected of involvement in the distribution of high-risk spyware technology raises serious questions that cannot be ignored: to what extent is there a crossover between business interests, political power networks, and state authority within Indonesia's digital surveillance ecosystem?

Furthermore, in various global contexts, similar technology has been repeatedly documented as an instrument of human rights violations, used to spy on journalists, activists, human rights defenders, and other vulnerable groups. If a similar pattern occurs in Indonesia, the presence of political actors in this spyware business chain has the potential to create systemic conflicts of interest and be dangerous to democracy.

Indonesia as a "Legal Grey Area" for Spyware Sales

Based on an investigative report published by Lighthouse Reports in October 2025, Indonesia is not only recorded as a user of highly intrusive spyware technology, but is also suspected of acting as an intermediary (middleman) in the distribution and use ecosystem of this surveillance software.[305]

To date, Indonesia lacks a comprehensive and explicit legal framework that regulates the trade, acquisition, and use of spyware technology. This regulatory vacuum has resulted in Indonesia being categorized as a country with a legal grey area, indirectly opening the door to the entry of high-risk surveillance technology from various companies with a track record of human rights violations without adequate oversight.

This situation is exacerbated by the fragmentation of existing regulations. Provisions regarding wiretapping and communications surveillance are currently

[304] Ministry of Law and Human Rights of the Republic of Indonesia, Company Profile of PT. Radika Karya Utama, 2020. Page 17, Accessed on 20 October 2025.
[305] Gabriel Geiger et al., "Surveillance Secrets," *Lighthouse Reports,* 23 May 2024, accessed 1 April 2026, https://www.lighthousereports.com/investigation/surveillance-secrets/ .

scattered across various sectoral legal instruments, namely Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), the Terrorism Law, and the Corruption Eradication Commission Law (KPK Law), each of which only regulates wiretapping in the context of specific cases with very limited judicial oversight.

More worryingly, this regulatory fragmentation has created unhealthy institutional competition. Several state institutions, including the Indonesian National Armed Forces (TNI), the Attorney General's Office, and the Indonesian National Police (Polri), appear to be competing to acquire and expand wiretapping authority, without adequate judicial oversight or transparent legal justification. Claims of "law enforcement" or "crime prevention," often used as a shield of legitimacy by these institutions, require serious criticism.

Several findings indicate that surveillance technology acquired in the name of law enforcement, in practice, has been used far beyond its intended boundaries, including political surveillance, the suppression of civil liberties, and the targeting of groups unrelated to any criminal activity. The legitimacy of the growing use of spyware actually threatens the foundations of international human rights law, particularly the principles of necessity and proportionality. Even in the handling of serious crimes, the use of this tool is difficult to justify legally as long as more proportionate alternative surveillance methods exist. Essentially, the surveillance capacity of spyware cannot be reconciled with individual privacy rights, the presumption of innocence, or the values that underpin a democratic society.[306]

Meanwhile, the recently enacted Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) does not specifically address the use of spyware by state actors. The absence of a single law comprehensively regulating wiretapping creates a legal vacuum that is exploited by various parties, both state and non-state actors.

In the context of international trade, the absence of strict export-import

[306] Bojan Perkov et al., *A Privacy Nightmare: Understanding Spyware,* (Share Foundation, 2025), p. 57.

regulations for dual-use technology in Indonesia makes the country a strategic target market for global spyware companies. Technologies internationally classified as dual-use, that is, technologies that can be used for both civilian and military purposes, should be subject to strict export control mechanisms as stipulated in the Wassenaar Arrangement, a multilateral export control regime that regulates the transfer of conventional and dual-use technology. However, the weak implementation of similar mechanisms in Indonesia as the recipient country creates a dangerous regulatory asymmetry.

Furthermore, the pattern identified in this study, where spyware products are disguised in shipping documents as ordinary commercial goods such as USB sticks, CPUs, monitors, pelican cases, and textile backpacks, indicates that actors in the surveillance technology distribution chain are deliberately exploiting weaknesses in Indonesia's customs classification system. The lack of adequate technical capacity at customs and export-import regulatory levels to identify disguised dual-use technology makes Indonesia vulnerable to the smuggling of surveillance technology, shielded by a facade of administrative legality.

This situation ultimately creates a dangerous paradox: the state is present as a major purchaser of spyware technology, while simultaneously absent as an effective regulator. Without a comprehensive legal framework, independent oversight mechanisms, and transparency in the procurement of surveillance technology, Indonesia not only becomes a legal grey area in the global spyware trade but also has the potential to become a laboratory of impunity for digital surveillance practices that violate human rights.

J. Postscript

J.1. Conclusion

The widespread use of surveillance technology has brought human rights to its nadir. Instruments originally designed for national security are now frequently misused to target human rights defenders. A poorly regulated private surveillance industry has created a market for abuse of power that threatens

citizens' fundamental rights. Efforts to regulate the surveillance industry globally also face significant challenges due to the secretive and complex nature of the spyware industry.

This characteristic is also evident in the procurement and use of spyware in Indonesia. Based on a review of government procurement documents and related corporate documents, this research found that surveillance equipment acquisitions involve not only major global vendors but also a network of supporting entities that provide operational infrastructure and geolocation tracking technology. The presence of this network of specialist providers allows surveillance activities to operate effectively under the radar of public scrutiny.

The complexity of tracking supply chains and technology procurement stems from a lack of accountability and a culture of secrecy in intelligence procurement. The use of local intermediary entities within the state procurement system often creates an administrative layer that effectively isolates the identity of the original technology provider from publicly accessible documents. This layered structure, coupled with the intertwined political and economic interests within the distribution channels, underscores the difficulty of controlling the control of intelligence tools operating in a regulatory vacuum.

In the regulatory context, Indonesia exists in a "legal grey area." The absence of independent oversight mechanisms and strict judicial control over the procurement of wiretapping devices makes Indonesia an open market for the spread of spyware. Without progressive policy reform, the gap between the state's extensive monitoring capacity and the protection of citizens' rights will continue to widen, threatening the rule of law and the future of digital justice.

J. 2. Recommendations

To ensure accountability for spyware use, strengthening policies is necessary, both through legislation, regulations, and even the use of public funds, including human rights-based procurement of goods and services. Optimizing e-procurement and strict oversight are also prerequisites for strengthening

transparency in the procurement of such devices. The government must prevent corruption, protect human rights from spyware abuse, and increase public trust in the use of cybersecurity technology. Therefore, this research recommends:

1) Developing specific regulations regarding the procurement and use of spyware, including device classification, criteria for user institutions, and human rights protection standards.

2) Requiring transparent procurement mechanisms through the government's e-procurement system, with a special category for surveillance technology that requires cross-agency permits.

3) Strengthening independent oversight by the House of Representatives (DPR), the Financial Supervisory Agency (BPK), the Indonesian Ombudsman (ORI), the National Human Rights Commission (Komnas HAM), the Prosecutorial Commission, and the National Police Commission (Kompolnas) over every spyware procurement contract to ensure legal and human rights compliance. Furthermore, the role of the Witness and Victim Protection Agency (LPSK) is also needed in cases where there are victims of spyware technology.

4) Requiring technology platforms like Apple, Meta, and Google to legally, through the courts, open access to device forensic data to verified victims and independent investigative bodies if there is sufficient preliminary evidence of spyware infection, in order to address the structural inequality in evidence that has been a major obstacle for victims in obtaining justice.

5) Applying the principle of necessity and proportionality, where spyware may only be used for legitimate law enforcement, is limited in time, and has court approval.

6) Establishing a mechanism for regular audits of the effectiveness, costs and human rights impacts of spyware use, as well as public reporting obligations in the form of non-technical summaries.

Bibliography

Access Now. "Exiled, Then Spied on: Civil Society in Latvia, Lithuania, and Poland Targeted With Pegasus Spyware - Access Now," 30 May 2024. https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

———."Access Now tells the 9th Circuit Court: NSO Group cannot escape accountability in U.S. courts." 23 December 2020. https://www.accessnow.org/press-release/nso-group-whatsapp-lawsuit-civil-society-amicus-brief/.

Afrose, Samia. "Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine." Bachelor's thesis, Harvard University, 2025.

Alam, Nur. "Konstitusionalitas Penyadapan (Interception) Dengan Peraturan Pemerintah Dari Sudut Pandang Perlindungan Hak Asasi Manusia." *Jatiswara* 27, no. 3 (November 2012).

Albanese, Francesca. *From economy of occupation to economy of genocide*. Laporan Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967. UN Doc. A/HRC/59/23. 2 July 2025.

Alfarizi, M. Khory. "Fakta-Fakta Pegasus, Spyware Canggih Yang Disebut Masuk Indonesia." *Tempo*, 20 June 2023. https://www.tempo.co/politik/fakta-fakta-pegasus-spyware-canggih-yang-disebut-masuk-indonesia-175195.

Aliansi Jurnalis Independen. "Jelang Pemilu 2024, Perlu Regulasi Penggunaan Alat Sadap seperti Pegasus." *Aji.or.id*. 23 June 2023.

https://www.aji.or.id/informasi/jelang-pemilu-2024-perlu-regulasi-penggunaan-alat-sadap-seperti-pegasus.

Allsop, Jon. "Around the World in (at Least) Eight Court Cases Involving Pegasus and the Press." Columbia Journalism Review, 14 February 2023. https://www.cjr.org/the_media_today/pegasus_spyware_court_cases.php.

Amnesty International. "A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia," 2024.

———. "When Is Targeted Surveillance Wrong?," 10 August 2023. https://www.amnesty.org/en/latest/campaigns/2020/10/stopspying/.

———. *A Web of Surveillance: Unravelling a Murky Network of Spyware Exports to Indonesia*. Index: ASA 21/7974/2024. 20 May 2024. https://www.amnesty.org/en/documents/asa21/7974/2024/en/.

———. T*he Predator Files: Caught in the Net*. Index: ACT 10/7245/2023, 9 October 2023. https://www.amnesty.org/en/documents/act10/7245/2023/en/.

———. "Thailand: Dismissal of Landmark Case a Critical and Alarming Setback in Fight Against Unlawful Use of Spyware." 21 November 2024. https://www.amnesty.org/en/latest/news/2024/11/thailand-dismissal-of-landmark-case-a-critical-and-alarming-setback-in-fight-against-unlawful-use-of-spyware/.

Amnesty International Security Lab. "Forensic Methodology Report: How to Catch NSO Group's Pegasus." *Amnesty International*. 18 July 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/.

———. “Technical Deep Dive into Intellexa Alliance Surveillance Products.” *Amnesty International*. 9 October 2023. https://securitylab.amnesty.org/latest/2023/10/technical-deep-dive-into-intellexa-alliance-surveillance-products/.

Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO). “Operating From the Shadows: Inside NSO Group’s Corporate Structure.” Amnesty International Ltd, 2021.

Amnesty International UK. “Evidence of Global Opposition to US Mass Surveillance,” 16 January 2026. https://www.amnesty.org.uk/mass-surveillance-us-nsa-edward-snowden-gchq.

Anderson, Stuart Joseph. “Comparing Section 889’s Huawei Ban and the Cybersecurity Maturity Model Certificate: The Challenge of Pursuing Cybersecurity Through Friend-Shoring.” *Public Contract Law Journal* 54, no. 2 (2025).

Angiolillo, Fabio, Ana Good God, and Staffan I. Lindberg. “DEMOCRACY REPORT 2025: 25 Years of Autocratization – Democracy Trumped?” V-Dem Institute, March 2025.

Anugrahanto, Nino Citra, and Kurnia Yunita. “Satu Dekade Tren Indeks Demokrasi Indonesia Menurun.” *Kompas.id*, 5 March 2025. https://www.kompas.id/artikel/satu-dekade-tren-indeks-demokrasi-indonesia-menurun.

Arquillière, Maxime, et al. *Predators for Hire: A Global Overview of Commercial Surveillance Vendors*. Sekoia, 2025. https://blog.sekoia.io/predators-for-hire-a-global-overview-of-commercial-surveillance-vendors/.

Article19. “Slovakia: Use of Pegasus a Threat to Democracy and Human Rights,” 9 September 2024. https://www.article19.org/resources/slovakia-use-of-pegasus-a-threat-to-democracy-and-human-rights/#:~:text=The%20European%20Union%20Agency%20for,use%20of%20Pegasus%20in%20Slovakia.

Asia Pacific Defence Reporter. “Indonesia Defense Expenditure to Reach $9.7 Billion by 2028.” *Asia Pacific Defence Reporter*. 31 August 2023. https://asiapacificdefencereporter.com/indonesia-defense-expenditure-to-reach-9-7-billion-by-2028/

BBC. “Pegasus: Who Are the Alleged Victims of Spyware Targeting?,” 22 July 2021. https://www.bbc.com/news/world-57891506.

———. “Pegasus: Spyware Sold to Governments ‘Targeted Activists’.” 19 July 2021. https://www.bbc.com/news/world-57891506.

BDS Movement. “The Dangerous Rise of Military-Grade Spyware – a Global Day of Action,” 18 June 2025. Accessed on 31 December 2025. https://bdsmovement.net/Global-Day-Action-Against-Spyware.

Bień-Kacała, Agnieszka. “Pegasus contra democratic process: experience from Europe.” Dalam *Artificial Intelligence and International Human Rights Law: Developing Standards for a Changing World*, edited by Michał Balcerzak and Julia Kapelańska-Pręgowska. Cheltenham: Edward Elgar Publishing Limited, 2024.

Bloch, Julie, Sukti Dhital, Rashmika Nedungadi, and Nikki Reisch. “CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent.” Just Security, 15 May 2019. https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent/.

Bromley, Mark, and Giovanna Maletta. *Export Controls and Spyware: Enhancing Oversight, Transparency and Restraint*. SIPRI Report. Stockholm: SIPRI, September 2025. http://doi.org/10.55163/GVXO6716.

Cardillo, Maira, Sina Fischer, and Aditi Kekre. *Targeting, Infecting, Surveilling, Harming A Criminal and Human Rights Context: Mapping the Impact and Harm of Spyware on People*. Geneva Graduate Institute and CyberPeace Institute, 2023.

Carpenter, Chris. "Symposium on Forensic and Counter-Forensic Approaches to International Law: Digital Evidence and the Gaze – a Conceptual Framework for Analyzing Digital Evidence Through a Foucauldian Lens." Opinio Juris, 16 March 2026. https://opiniojuris.org/2025/12/10/symposium-on-forensic-and-counter-forensic-approaches-to-international-law-digital-evidence-and-the-gaze-a-conceptual-framework-for-analyzing-digital-evidence-through-a-foucauldian-lens/.

Cecco, Leyland. "Spyware Is Huge Threat to Global Human Rights and Democracy, Expert Warns." *The Guardian*, 10 August 2022. https://www.theguardian.com/world/2022/aug/09/spyware-canada-threat-democracy-human-rights.

Chan, Anna W. "The Need for a Shared Responsibility Regime Between State and Non-State Actors to Prevent Human Rights Violations Caused by Cyber-Surveillance Spyware." *The Brooklyn Journal of International Law* 44, no. 2 (2019). https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/7/.

Chin-Rothmann, Caitlin. "Cyber Mercenaries: Limiting Government Use of Commercial Spyware." Georgetown Journal of International Affairs,

4 September 2024. https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/.

Cowley, Ruth. "Kiobel's Impact on Disputes in International Law." *Norton Rose Fulbright*, May 2013. https://www.nortonrosefulbright.com/en/knowledge/publications/94bc936c/kiobels-impact-on-disputes-in-international-law.

Dragonfly Intelligence. "Risks to organisations from spyware," 27 June 2024. https://dragonflyintelligence.com/news/global-risks-to-organisations-from-spyware/.

Deibert, Ronald J. *Chasing Shadows: Cyber Espionage, Subversion, and the Global Fight for Democracy*. Toronto: Simon & Schuster, 2025.

Dumbrava, Costica. *Impact of the Use of Spyware on Fundamental Rights*. Brussels: European Parliamentary Research Service, 2023. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf,

Feldstein, Steven. "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, 23 December 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661.

———. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace, 17 September 2019. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance.

Feldstein, Steven, and Brian Kot. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace, March 2023.

———. “Mapping the Shadowy World of Spyware and Digital Forensics Sales.” Carnegie Endowment for International Peace, 27 February 2023. https://carnegieendowment.org/features/commercial-spyware?lang=en.

Fidler, Mailyn. “Sanctions for Spyware.” Lawfare, 13 June 2024. https://www.lawfaremedia.org/article/sanctions-for-spyware.

Ní Aoláin, Fionnuala, and Adriana Edmeades Jones. “Spyware Out of the Shadows: The Need for a New International Regulatory Approach.” *Just Security*. 15 May 2023. https://www.justsecurity.org/86558/spyware-out-of-the-shadows-the-need-for-a-new-international-regulatory-approach/.

Fortinet. “What Is Spyware? Definition, Types and Protection | Fortinet,” n.d. https://www.fortinet.com/resources/cyberglossary/spyware.

Gamma Group. “Remote Monitoring and Infection Solutions: FinSpy.” *WikiLeaks Spyfiles*. 1 December 2011. https://wikileaks.org/spyfiles/docs/gamma/289_remote-monitoring-and-infection-solutions-finspy.html.

Geiger, Gabriel, et al. “Surveillance Secrets.” *Lighthouse Reports*. 23 May 2024. https://www.lighthousereports.com/investigation/surveillance-secrets/.

Global Justice Clinic. “Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights,” 1 March 2019.

Guterl, Fred. “Special Report: When Spyware Turns Phones Into Weapons.” Committee to Protect Journalists, 13 October 2022.

https://cpj.org/reports/2022/10/when-spyware-turns-phones-into-weapons/.

Hanan Elatr Khashoggi v. NSO Group Technologies Limited, et al. No. 23-2234. United States Court of Appeals for the Fourth Circuit, 21 May 2025. https://law.justia.com/cases/federal/appellate-courts/ca4/23-2234/23-2234-2025-05-21.html.

Hever, Alexandra. "The Price of Inequality: Why Tax Is a Human Rights Issue." *HRRC* (blog), 27 June 2025. https://www.humanrightsresearch.org/post/the-price-of-inequality-why-tax-is-a-human-rights-issue.

Hidayat, Bagja. "Indonesia 2026: Makin Riuh Makin Represif." *Tempo*, 4 January 2026. https://www.tempo.co/prelude/sampul-tempo-edisi-khusus-indonesia-2026-2104222.

Hiebert, Kyle Volpi. "The Growing Global Spyware Industry Must Be Reined In." *CIGI*, 27 March 2023. https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/.

Hindin, Doron. "Can Export Controls Tame Cyber Technology?: An Israeli Approach." *Lawfare*, 12 February 2016. https://www.lawfaremedia.org/article/can-export-controls-tame-cyber-technology-israeli-approac

Horak, Steven. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023.

Hrle, Vladimir. "Corporate Responsibility in the Age of Surveillance and Transnational Repression: Legal Obligations and Human Rights Due

Diligence.” International Bar Association, 21 August 2025. https://www.ibanet.org/corporate-responsibility-in-age-of-surveillance-and-transnational-repression-legal-obligations-human-rights-due-diligence.

International Commission of Jurists. “Digital Technologies and Human Rights: a Legal Framework.” International Commission of Jurists, May 2022.

In ‘t Veld, Sophie (Rapporteur). *Draft Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware (2022/2077(INI))*. European Parliament Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA). 8 November 2022.

———. “Spyware Regulation: Will the New European Commission Step Up?.” *Digital Frontlines*. 31 January 2025. https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/,

Kaye, David. “David Kaye: Here’s What World Leaders Must Do About Spyware.” Committee to Protect Journalists, 13 October 2022. https://cpj.org/2022/10/david-kaye-what-world-leaders-must-do-about-spyware/.

Kaye, David, and Sarah McKune. “The Scourge of Commercial Spyware—and How to Stop It.” *Lawfare*, 25 August 2023. https://www.lawfaremedia.org/article/the-scourge-of-commercial-spyware-and-how-to-stop-it.

Kotliar, Dan M., and Elinor Carmi. “Keeping Pegasus on the Wing: Legitimizing Cyber Espionage.” *Information, Communication & Society* 27, no. 8 (2024): 1499–1529. https://doi.org/10.1080/1369118X.2023.2245873

Kirchgaessner, Stephanie. "Saudis Behind NSO Spyware Attack on Jamal Khashoggi's Family, Leak Suggests." *The Guardian*, 18 July 2021. https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus.

Kirchgaessner, Stephanie, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani, Michael Safi, and Luke Hoyland. "Revealed: Leak Uncovers Global Abuse of Cyber-surveillance Weapon." *The Guardian*, 18 July 2021. https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

Korzak, Elaine. "Managing Commercial Spyware Through Export Controls: Lesson Learned from the Wassenaar Experience." Center for Long-Term Cybersecurity (CLTC) UC Berkeley, March 2025.

———."Regulating Commercial Spyware Through Export Controls." *Lawfare*, 10 December 2025. https://www.lawfaremedia.org/article/regulating-commercial-spyware-through-export-controls.

Lighthouse Reports. "Surveillance Secrets." *Lighthouse Reports*. 23 May 2024. https://www.lighthousereports.com/investigation/surveillance-secrets/.

Loewenstein, Antony. "How Palestine Became Israel's Spyware Test-bed." New Internationalist, 19 October 2023. https://newint.org/features/2023/10/02/spy-games.

Lourens, Cecile. "Surveillance at the Intersection of Technology, Business and Politics: A Case Study of Pegasus Spyware." *Diggit Magazine*, 20 May 2022.

https://www.diggitmagazine.com/articles/surveillance-intersection-technology-business-and-politics-case-study-pegasus-spyware.

Marczak, Bill, et al. "Mapping FinFisher's Continuing Proliferation." *Citizen Lab*. 15 October 2015. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/#51.

Marquis-Boire, Morgan, et al. "You Only Click Twice: FinFisher's Global Proliferation." *Citizen Lab*. 13 March 2013. https://citizenlab.ca/research/you-only-click-twice-finfishers-global-proliferation-2/#1.

Marczak, Bill, and John Scott-Railton. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against A UAE Human Rights Defender." *The Citizen Lab*, 24 August 2016. https://citizenlab.ca/research/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marzocchi, Ottavio, and Martina Mazzini. *Pegasus and Surveillance Spyware*. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, 2022.

Megiddo, Tamar. "Spyware Exports: Recognizing the Limits of Human Rights Law." SSRN, 23 December 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5123661.

Monahan, Torin, and David Murakami Wood. "Introduction: Surveillance Studies as a Transdisciplinary Endeavor." Dalam *Surveillance Studies: A Reader*, edited by Torin Monahan and David Murakami Wood. Oxford: Oxford University Press, 2018.

Morris, Daniel, and Cathrine Bloch Veiberg. "Public Procurement as a Tool to Address Human Rights Risk in the Use of Digital Technology to

Deliver Essential Public Services." Copenhagen K: The Danish Institute for Human Rights, February 2024.

Ní Aoláin, Fionnuala. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. UN Human Rights Special Procedures. April 2023.

———.*Global Study on the Impact of Counter-Terrorism Measures on Civil Society and Civic Space*. Laporan Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. UN Doc. A/HRC/52/39. 1 March 2023.

———. *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*. UN Doc. A/HRC/52/39. 1 March 2023.

Office of the United Nations High Commissioner for Human Rights (OHCHR). *Mapping report: human rights and new and emerging digital technologies*. UN Doc. A/HRC/56/45. 20 August 2024.

———. *The Right to Privacy in the Digital Age*. UN Doc. A/HRC/60/45. 29 August 2025.

Papaprodromou, Lazaros G. *Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach*. Office of the United Nations High Commissioner for Human Rights (OHCHR), 2023.

Papademetriou, George T. "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry." *Harvard Human Rights Journal* 36 (2023).

Perkov, Bojan, et al. *A Privacy Nightmare: Understanding Spyware*. Share Foundation, 2025.

Prashad, Vijay, and Ubai Al-aboudi. "How the World Enriches from the Blood of the Palestinians." Progressive International, 17 November 2025. https://progressive.international/wire/2025-11-17-how-the-world-enriches-from-the-blood-of-the-palestinians/en/.

Putra, Han Revanda. "Investigasi Tempo Ungkap Perusahaan Israel Diduga Pasok Spyware ke Indonesia Sejak 2017." *Tempo.co*. 20 June 2024. https://www.tempo.co/arsip/investigasi-tempo-ungkap-perusahaan-israel-diduga-pasok-spyware-ke-indonesia-sejak-2017-62228.

Qandeel, Mais, and Özgün Erdener Topak. "Genocidal Surveillant Assemblage in Palestine: A Socio-Legal Analysis." *Journal of Genocide Research*, October 2025. https://doi.org/10.1080/14623528.2025.2567372.

Rahayu, Kurnia Yunita and Hidayat Salam. "Sejalan dengan Visi Prabowo, Anggaran Pertahanan Naik Jadi Rp 165 Triliun." *Kompas.id*. 16 August 2024. https://www.kompas.id/artikel/sejalan-dengan-visi-prabowo-anggaran-pertahanan-naik-jadi-rp-165-triliun.

Ramadhan, Fahmi. "Teken Nota Kesepakatan dengan Provider, Kejagung Bisa Pasang Alat Sadap untuk Kumpulkan Data." *Tribunnews.com*. 26 June 2025.https://www.tribunnews.com/nasional/2025/06/26/teken-nota-kesepakatan-dengan-provider-kejagung-bisa-pasang- alat-sadap-untuk-kumpulkan-data.

Razzak, Abdul, Masashi Crete-Nishihata, and Ron Deibert. "Reckless VI: Mexican Journalists Investigating Cartels Targeted With NSO Spyware Following Assassination of Colleague." The Citizen Lab, 27 November 2018. https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-

targeted-nso-spyware-following-assassination-colleague/#:~:text=Key%20Findings,to%20prevent%20the%20continuing%20abuse.

Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126 (1934).

Richard, Laurent, and Sandrine Rigaud. *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy*. New York: Henry Holt and Co., 2023.

Rizaldi, Bagus Ahmad. "Anggota DPR Sebut BIN Perlu Investasi Teknologi Intelijen Terkini." *Antaranews.com*. 21 May 2025. https://www.antaranews.com/berita/4820745/anggota-dpr-sebut-bin-perlu-investasi-teknologi-intelijen-terkini.

Roberts, Jen, Trey Herr, Nitansha Bansal, Nancy Messieh, Emma Taylor, Jean Le Roux, Sopo Gelava, and Atlantic Council. "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights." Atlantic Council, 4 September 2024. https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/.

Rueckert, Phineas. "Pegasus: The New Global Weapon for Silencing Journalists." Forbidden Stories, 18 July 2021. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/.

Santos, Edmarverson A. "Human Rights and the Global Digital Surveillance Infrastructure." *Diplomacy and Law* (blog), 3 July 2025. https://www.diplomacyandlaw.com/post/human-rights-and-the-global-digital-surveillance-infrastructure.

Sartor, Giovanni, and Andrea Loreggia. “The Impact of Pegasus on Fundamental Rights and Democratic Processes.” European Union, 2022.

Scott-Railton, John, Bill Marczak, Irene Poetranto, Bahr Abdul Razzak, Sutawan Chanprasert, and Ron Deibert. “GeckoSpy: Pegasus Spyware Used Against Thailand’s Pro-Democracy Movement - the Citizen Lab.” The Citizen Lab, 7 July 2022. https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/.

Sexton, Mike. “What Is Spyware and Why Should Policymakers Care?” Third Way, 9 March 2023. https://www.thirdway.org/memo/what-is-spyware-and-why-should-policymakers-care.

Silberman, Michael. “Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability.” *Georgetown Law Technology Review* 8, no. 1 (2024).

Sodiq, Mohamad Djafar, et al. “Kebijakan dan Regulasi Spionase Siber di Indonesia.” *IDEAS: Jurnal Pendidikan, Sosial, dan Budaya* 10, no. 4. November 2024. https://jurnal.ideaspublishing.co.id /index.php/ideas/ article/ view/1909/799.

Sooknanan, Isabella S. S. “Digital Authoritarianism and the Expansion of the Global Surveillance State.” Senior thesis, Fordham University, 2023. https://research.library.fordham.edu/cgi/viewcontent.cgi?article=1138&context=international_senior.

Šturmová, Barbora. “Pegasus Spyware Targeted Over 1,400 WhatsApp Users, Including in Hungary and Czechia, Court Documents Show.” *VSquare*, 20 November 2024. https://vsquare.org/pegasus-spyware-hacking-whatsapp-meta-hungary-czech-republic/.

Tax Justice Network. “Inequalities and Democracy and Human Rights,” 13 November 2020. https://taxjustice.net/topics/inequalities-and-democracy-and-human-rights/.

Tempo. “Apa Kabar RUU Penyadapan?.” 26 June 2021. https://www.tempo.co/hukum/apa-kabar-ruu-penyadapan-823459.

The Initiative for Human Rights Principles in Fiscal Policy. *Principles for Human Rights in Fiscal Policy*.

Tim Privacy International and ELSAM. *Privasi 101: Panduan Memahami Privasi, Perlindungan Data, dan Surveilans Komunikasi*. Jakarta: ELSAM, 2015.

UN General Assembly. *The Right to Privacy in the Digital Age*. UN Doc. A/RES/73/179. 17 December 2018.

UN Human Rights Council. *The Rights to Freedom of Peaceful Assembly and of Association*. Resolusi A/HRC/50/L.16. 30 June 2022.

———. *The Rights to Freedom of Peaceful Assembly and of Association*. Resolusi A/HRC/50/L.20. 4 July 2022.

———. *Annex to the Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions: Investigation into the Unlawful Death of Mr. Jamal Khashoggi*. A/HRC/41/CRP.1. 19 June 2019.

UN Interregional Crime and Justice Research Institute (UNICRI) and UN Office of Counter-Terrorism (UNOCT). *Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks*. 2024.

Uren, Tom. “Amnesty Flags Possible Spyware Abuse in Indonesia.” *Lawfare*, 17 May 2024. https://www.lawfaremedia.org/article/amnesty-flags-possible-spyware-abuse-in-indonesia

Veld, Sophie in 't. "An Inquiry on Spyware in the EU Revealed Abuses by Member States. Now What?" Digital Front Lines, n.d. https://digitalfrontlines.io/2025/01/31/spyware-regulation-european-commission/.

Vijayan, Suchitra. "Technologies of Genocide: How Big Tech Profits From Mass Annihilation." The Polis Project, 20 August 2025. https://thepolisproject.com/listen/technologies-of-genocide-how-big-tech-profits-from-mass-annihilation/.

Yepes, Rodrigo Uprimny, and Mariana Matamoros. "A Human Rights-based Approach to Tax Systems." *Dejusticia*, October 2024. https://www.dejusticia.org/en/a-human-rights-based-approach-to-tax-systems/.

Zaki, M. Faiz. "Amnesty International Ungkap Polri Impor Alat Sadap, Ini Kata Pakar Kepolisian Soal SOP Penyadapan." *Tempo.co*. 20 June 2024. https://www.tempo.co/hukum/amnesty-international-ungkap-polri-impor-alat-sadap-ini-kata-pakar-kepolisian-soal-sop-penyadapan-61122.

Zvi, Ronnie Rosen. "Managing Risky Business – the International Regulatory Framework of Spyware Companies: Where It Is Lacking and Where It Is Heading." Georgetown Law, 30 January 2023. https://www.law.georgetown.edu/ctbl/blog/managing-risky-business-the-international-regulatory-framework-of-spyware-companies-where-it-is-lacking-and-where-it-is-heading/.

Profile



Since its establishment on August 14, 1993, ELSAM has developed a strategy that combines the working methods of a think tank and a human rights movement organization in its operations. This distinctive character makes ELSAM unique as a movement-based think tank, with two primary focuses: conducting studies using a rights-based approach and engaging in policy advocacy. ELSAM strives to promote evidence-based policymaking to strengthen the respect for, fulfillment of, and protection of human rights.

The establishment of ELSAM was intended to realize a social order grounded in the values of human rights, justice, and democracy. To achieve this goal, ELSAM develops at least four main areas of activity:

1. Human rights studies and knowledge production to support policy advocacy;
2. Mainstreaming human rights in policymaking;
3. Legal advocacy to encourage policy reform, including through strategic litigation; and
4. Organizing various human rights education programs with diverse topics and target audiences.

These activities are primarily implemented through several strategic thematic areas, including:

1. Human Rights and Technology — responding to the rapid pace of digital technological innovation and its broad impact on human rights;

2. Human Rights and Business — recognizing the increasing role of corporations in shaping relationships between rights holders and duty bearers;
3. Human Rights and the Environment — emphasizing environmental sustainability as an integral part of human rights;
4. Fundamental Freedoms — especially freedom of expression, freedom of religion/belief, and freedom of assembly/association;
5. Transitional Justice — promoting accountability and resolution for past human rights violations.

For more than two decades, ELSAM has contributed significantly to promoting the adoption and implementation of human rights in Indonesia, ranging from the ratification of international human rights conventions to the drafting of numerous laws. Post-Reformasi laws such as the Truth and Reconciliation Commission Law, the Witness and Victim Protection Law, and most recently the Personal Data Protection Law, were all areas in which ELSAM played a direct role during the legislative process.

Currently, ELSAM is actively advocating for policies that respond to the rapid advancement of digital technology. ELSAM's contribution to promoting digital policies centered on a human-centric approach was publicly recognized through the Good ID Award 2020 in the Security category, a global award recognizing individuals and civil society organizations that contribute significantly to the development of sound digital governance policies.

ELSAM is also actively involved in strengthening Indonesia's human rights institutions, such as the National Human Rights Commission (Komnas HAM) and the Witness and Victim Protection Agency (LPSK), while also ensuring the consistent implementation of human rights through support for optimizing the National Human Rights Action Plan (RAN HAM). ELSAM continuously strengthens the capacity of various human rights stakeholders, both within the state and civil society. It organizes human rights courses on a wide range of topics for human

rights defenders, public interest lawyers, policymakers, law enforcement officers, and corporations.

Toward 2045, ELSAM envisions the following long-term transformative goal:

> **"An empowered, inclusive, equal, and technologically capable Indonesian society within a human rights and democratic order for social and ecological justice."**

This vision is translated into the 2025–2030 Strategic Plan, consisting of five Intermediate Outcomes:

1. Building the foundation for political alliances with reform-minded actors within state institutions;
2. Strengthening critical perspectives among civil society regarding policies in the digital sphere;
3. Providing knowledge infrastructure to foster human rights activism in the digital environment;
4. Developing new constituencies with a human rights perspective as citizens in the digital sphere;
5. Building new narratives that support human rights agendas and victims' rights in the digital environment.

Institute for Policy Research and Advocacy (ELSAM)
Address: Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510, Indonesia
Phone: (+62 21) 797 2662 **Email:** office@elsam.or.id **Website:** elsam.or.id
Social Media: **IG and X** @elsamnews **Facebook**: elsamjkt **YouTube**: Perkumpulan ELSAM